AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

PROTECTING THE ELECTRIC GRID: H.R. 2165, THE "BULK POWER SYSTEM PROTECTION ACT OF 2009," AND H.R. 2195

HEARING

BEFORE THE

SUBCOMMITTEE ON ENERGY AND ENVIRONMENT

OF THE

COMMITTEE ON ENERGY AND COMMERCE
HOUSE OF REPRESENTATIVES

ONE HUNDRED ELEVENTH CONGRESS

FIRST SESSION

OCTOBER 27, 2009

Serial No. 111–77

Printed for the use of the Committee on Energy and Commerce

energycommerce.house.gov

U.S. GOVERNMENT PRINTING OFFICE

74–848 WASHINGTON : 2012

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2104 Mail: Stop IDCC, Washington, DC 20402–0001

COMMITTEE ON ENERGY AND COMMERCE

HENRY A. WAXMAN, California, *Chairman*

JOHN D. DINGELL, Michigan
Chairman Emeritus
EDWARD J. MARKEY, Massachusetts
RICK BOUCHER, Virginia
FRANK PALLONE, JR., New Jersey
BART GORDON, Tennessee
BOBBY L. RUSH, Illinois
ANNA G. ESHOO, California
BART STUPAK, Michigan
ELIOT L. ENGEL, New York
GENE GREEN, Texas
DIANA DEGETTE, Colorado
Vice Chairman
LOIS CAPPS, California
MICHAEL F. DOYLE, Pennsylvania
JANE HARMAN, California
TOM ALLEN, Maine
JANICE D. SCHAKOWSKY, Illinois
CHARLES A. GONZALEZ, Texas
JAY INSLEE, Washington
TAMMY BALDWIN, Wisconsin
MIKE ROSS, Arkansas
ANTHONY D. WEINER, New York
JIM MATHESON, Utah
G.K. BUTTERFIELD, North Carolina
CHARLIE MELANCON, Louisiana
JOHN BARROW, Georgia
BARON P. HILL, Indiana
DORIS O. MATSUI, California
DONNA M. CHRISTENSEN, Virgin Islands
KATHY CASTOR, Florida
JOHN P. SARBANES, Maryland
CHRISTOPHER S. MURPHY, Connecticut
ZACHARY T. SPACE, Ohio
JERRY MCNERNEY, California
BETTY SUTTON, Ohio
BRUCE L. BRALEY, Iowa
PETER WELCH, Vermont

JOE BARTON, Texas
Ranking Member
RALPH M. HALL, Texas
FRED UPTON, Michigan
CLIFF STEARNS, Florida
NATHAN DEAL, Georgia
ED WHITFIELD, Kentucky
JOHN SHIMKUS, Illinois
JOHN B. SHADEGG, Arizona
ROY BLUNT, Missouri
STEVE BUYER, Indiana
GEORGE RADANOVICH, California
JOSEPH R. PITTS, Pennsylvania
MARY BONO MACK, California
GREG WALDEN, Oregon
LEE TERRY, Nebraska
MIKE ROGERS, Michigan
SUE WILKINS MYRICK, North Carolina
JOHN SULLIVAN, Oklahoma
TIM MURPHY, Pennsylvania
MICHAEL C. BURGESS, Texas
MARSHA BLACKBURN, Tennessee
PHIL GINGREY, Georgia
STEVE SCALISE, Louisiana

SUBCOMMITTEE ON ENERGY AND ENVIRONMENT

EDWARD J. MARKEY, Massachusetts, *Chairman*

MICHAEL F. DOYLE, Pennsylvania
G.K. BUTTERFIELD, North Carolina
CHARLIE MELANCON, Louisiana
BARON P. HILL, Indiana
DORIS O. MATSUI, California
JERRY McNERNEY, California
PETER WELCH, Vermont
JOHN D. DINGELL, Michigan
RICK BOUCHER, Virginia
FRANK PALLONE, New Jersey
ELIOT L. ENGEL, New York
GENE GREEN, Texas
LOIS CAPPS, California
JANE HARMAN, California
CHARLES A. GONZALEZ, Texas
TAMMY BALDWIN, Wisconsin
MIKE ROSS, Arkansas
JIM MATHESON, Utah
JOHN BARROW, Georgia

DENNIS HASTERT, Illinois
Ranking Member
RALPH M. HALL, Texas
FRED UPTON, Michigan
ED WHITFIELD, Kentucky
JOHN SHIMKUS, Illinois
JOHN B. SHADEGG, Arizona
STEVE BUYER, Indiana
GREG WALDEN, Oregon
SUE WILKINS MYRICK, North Carolina
JOHN SULLIVAN, Oklahoma
MICHAEL C. BURGESS, Texas

CONTENTS

	Page
Hon. Edward J. Markey, a Representative in Congress from the Commonwealth of Massachussetts, opening statement	1
Hon. Fred Upton, a Representative in Congress from the State of Michigan, opening statement	32
Hon. John D. Dingell, a Representative in Congress from the State of Michigan, opening statement	33
Hon. John Shimkus, a Representative in Congress from the State of Illinois, prepared statement	34
Hon. Doris O. Matsui, a Representative in Congress from the State of California, opening statement	35
Hon. Cliff Stearns, a Representative in Congress from the State of Florida, opening statement	35
Hon. Jerry McNerney, a Representative in Congress from the State of California, opening statement	36
Hon. Tammy Baldwin, a Representative in Congress from the State of Wisconsin, opening statement	37
Hon. John Barrow, a Representative in Congress from the State of Georgia, opening statement	37
Hon. Gene Green, a Representative in Congress from the State of Texas, prepared statement	52
Hon. Michael C. Burgess, a Representative in Congress from the State of Texas, prepared statement	54

WITNESSES

Hon. Bennie G. Thompson, a Representative in Congress from the State of Mississippi, and Chairman, Committee on Homeland Security	
Prepared statement	38
Hon. James R. Langevin, a Representative in Congress from the State of Rhode Island, and Chairman, Subcommittee on Strategic Forces, House Armed Services Committee	
Prepared statement	58
Joseph McClelland, Director, Office of Electric Reliability, Federal Energy Regulatory Commission	63
Prepared statement	66
Patricia Hoffman, Principal Deputy Assistant Secretary, Office of Electricity, U.S. Department of Energy	78
Prepared statement	81
Answers to submitted questions	166
Garry A. Brown, Chairman, New York Public Service Commission	88
Prepared statement	91
David N. Cook, Vice President and General Counsel, North American Electric Reliability Corporation	110
Prepared statement	112
Answers to submitted questions	169
John DiStasio, General Manager and CEO, Sacramento Municipal Utility District	126
Prepared statement	128

SUBMITTED MATERIAL

H.R. 2165	3
H.R. 2195	19
Letter of November 10, 2009, from Mr. DiStasio to Subcommittee	160

PROTECTING THE ELECTRIC GRID: H.R. 2165, THE "BULK POWER SYSTEM PROTECTION ACT OF 2009," AND H.R. 2195

TUESDAY, OCTOBER 27, 2009

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON ENERGY AND ENVIRONMENT,
COMMITTEE ON ENERGY AND COMMERCE,
Washington, DC.

The subcommittee met, pursuant to call, at 9:37 a.m., in Room 2322, Rayburn House Office Building, Hon. Edward J. Markey [chairman of the subcommittee] presiding.

Present: Representatives Markey, Inslee, Butterfield, Matsui, McNerney, Dingell, Baldwin, Matheson, Barrow, Upton, Stearns, Shimkus, Blunt, Pitts, Walden, Sullivan, Burgess, Scalise, and Barton (ex officio).

Staff Present: Bruce Wolpe, Senior Advisor; John Jimison, Senior Counsel; Jeff Baran, Counsel; Caitlin Haberman, Special Assistant; Lindsay Vidal, Special Assistant; Earley Green, Chief Clerk; Mitchell Smiley, Special Assistant; Matt Eisenberg, Staff Assistant; Andrea Spring, Minority Professional Staff; Peter Spencer, Minority Professional Staff; Aaron Cutler, Minority Counsel; Amanda Mertens Campbell, Minority Counsel; and Garrett Golding, Minority Legislative Analyst.

OPENING STATEMENT OF HON. EDWARD J. MARKEY, A REPRESENTATIVE IN CONGRESS FROM THE COMMONWEALTH OF MASSACHUSETTS

Mr. MARKEY. Good morning. Welcome to the Subcommittee on Energy and Environment and to this very important hearing.

The Nation Academy of Engineering has called the North American electric grid the "supreme engineering achievement of the 20th century." The grid is one of our greatest strengths, but, if not properly protected, it could become one of our greatest weaknesses.

More than any other technology, the grid is the long pole in the tent of America's economy and national security. All of our Nation's critical systems—financial services, health care, telecommunications, transportation, water, defense, law enforcement, and so on—depend on the grid.

Remarkably, 99 percent of the electric energy used to power our military facilities, including critical strategic command assets, come from the commercially operated grid. Our dependence on the grid will only deepen as we move toward greater reliance on automation and information technology.

It has becoming increasingly clear in the last 2 years that the grid is vulnerable to cyber attacks and to other threats from terrorists, criminals, and hostile states. Over 2 years ago, the Department of Homeland Security revealed the so-called "Aurora vulnerability" through which hackers could use communications networks to physically destroy electric generators, transformers, and other critical assets.

We know that the cyber system controlling the grid and other critical infrastructure are continuously probed by outside parties. Just last week, the U.S.-China Commission reported on China's deep involvement in cyber espionage. In addition, new risks are coming to light, such as grid control systems vulnerability, to portable weapons that use high-powered radio frequency, or microwaves to destroy electronic equipment. Some of these vulnerabilities could worsen if we don't implement smart grid technologies in a smart way.

This past Thursday, I was joined by a number of other members of this subcommittee at a classified briefing on grid security. I assure you, the vulnerabilities of the grid are every bit as urgent as the weaknesses in transportation security that were so tragically revealed by the events of September 11th. A coordinated attack on the grid could literally shut down the U.S. economy, putting lives at risk and costing tens of billions of dollars. Moreover, unlike a storm knocking out power lines that can be replaced in a matter of days, an attack on the grid could result in damage requiring months or years to fix.

There is broad agreement that to meet these challenges we need new Federal authorities and mandates. The status quo for Federal regulation in this area, which relies exclusively on industry development or consensus reliability standards through the North American Electric Reliability Corporation, is inadequate.

That said, tough questions remain as to precisely what shape any new authorities and mandates should take. This morning we will consider two bills that address these issues: one sponsored by Mr. Barrow, which Chairman Waxman and I have cosponsored; and a second sponsored by Homeland Security Committee Chairman Bennie Thompson.

[The information follows:]

AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

I

111TH CONGRESS
1ST SESSION

H. R. 2165

To amend Part II of the Federal Power Act to address known cybersecurity threats to the reliability of the bulk power system, and to provide emergency authority to address future cybersecurity threats to the reliability of the bulk power system, and for other purposes.

IN THE HOUSE OF REPRESENTATIVES

APRIL 29, 2009

Mr. BARROW (for himself, Mr. MARKEY of Massachusetts, and Mr. WAXMAN) introduced the following bill; which was referred to the Committee on Energy and Commerce

---

A BILL

To amend Part II of the Federal Power Act to address known cybersecurity threats to the reliability of the bulk power system, and to provide emergency authority to address future cybersecurity threats to the reliability of the bulk power system, and for other purposes.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the "Bulk Power System Protection Act of 2009".

SEC. 2. FINDINGS.

The Congress finds that—

(1) it is in the public interest to require the Federal Energy Regulatory Commission to promptly order measures to address known cybersecurity threats to the reliability of the electric bulk power system; and

(2) the Commission must have the necessary emergency authority to respond promptly to future cybersecurity threats that could compromise reliability of the bulk power system.

SEC. 3. PROTECTION OF BULK POWER SYSTEM FROM CYBERSECURITY THREATS.

(a) IN GENERAL.—Part II of the Federal Power Act is amended by adding the following new section after section 215:

"SEC. 215A. EMERGENCY AUTHORITY TO ADDRESS CYBERSECURITY THREATS TO THE BULK POWER SYSTEM.

"(a) DEFINITIONS.—For purposes of this section:

"(1) The terms 'reliability standard', 'bulk power system', 'reliable operation', 'cybersecurity incident', 'Electric Reliability Organization', 'regional entity', and 'owners, users or operators' shall have the same meaning as when used in section 215.

"(2) The term 'cybersecurity threat' means that there is credible information or evidence of—

"(A) a likelihood of a malicious act that could disrupt the operation of those programmable electronic devices and communications networks including hardware, software and data that are essential to the reliable operation of the bulk power system; and

"(B) a substantial possibility of disruption to the operation of such devices and networks in the event of such a malicious act.

"(3) CLASSIFIED INFORMATION.—The term 'classified information' means any information that has been determined pursuant to Executive Order 12958, as amended, or successor orders, or the Atomic Energy Act of 1954, to require protection against unauthorized disclosure and that is so designated.

"(4) SENSITIVE CYBERSECURITY INFORMATION.—The term 'sensitive cybersecurity information' means unclassified information that, if an unauthorized disclosure is made, could be used in a malicious manner to impair the reliability or operations of the bulk power system or the supply of electricity to the bulk power system.

"(5) The term 'Secretary' means the Secretary of Energy.

"(b) INTERIM AUTHORITY TO ADDRESS EXISTING CYBERSECURITY THREATS.—

"(1) IN GENERAL.—After notice and opportunity for comment, and after consultation with appropriate governmental authorities in Canada and Mexico (subject to adequate protections against inappropriate disclosure of security-sensitive information), the Commission shall establish, by rule or order, within 120 days after enactment of this section, such measures or actions as are necessary to protect the reliability of the bulk power system against the cybersecurity threats resulting from—

"(A) the vulnerabilities identified in the June 21, 2007, communication to certain 'Electricity Sector Owners and Operators' from the North American Electric Reliability Corporation, acting in its capacity as the Electricity Sector Information Sharing and Analysis Center; and

"(B) related remote access issues.

Such measures or actions may be required of any owner, user, or operator of the bulk power system within the United States.

"(2) ADDITIONAL ORDERS.—Until such time as the interim reliability measures or actions ordered

1 under this subsection are replaced by cybersecurity
2 reliability standards developed, approved, and imple-
3 mented pursuant to section 215, the Commission
4 may issue additional orders to supplement the initial
5 rule or order issued under this subsection only if,
6 based on subsequent information or petition from an
7 affected entity, the Commission determines that
8 clarification or refinements to the originally ordered
9 measures or actions are necessary to ensure that the
10 threats are adequately and appropriately addressed.
11 Any such additional orders shall be preceded by no-
12 tice and opportunity for comment.

13 "(c) FUTURE EMERGENCIES INVOLVING IMMINENT
14 CYBERSECURITY THREATS.—

15 "(1) AUTHORITY TO ADDRESS IMMINENT CY-
16 BERSECURITY THREATS.—Whenever the President
17 issues and provides to the Commission (either di-
18 rectly or through the Secretary) a written directive
19 or determination that an imminent cybersecurity
20 threat to the reliability of the bulk power system ex-
21 ists, the Commission may on its own motion, with or
22 without notice, hearing, or report issue such orders
23 for emergency measures or actions as are necessary
24 in its judgment to protect the reliability of the bulk
25 power system against such threat.

"(2) CONSULTATION.—Before acting under this subsection, to the extent feasible, taking into account the nature of the threat and urgency of need for action, the Commission shall consult with appropriate governmental authorities in Canada and Mexico (subject to adequate protections against inappropriate disclosure of security-sensitive information), entities described in paragraph (3), and officials at other Federal agencies, including the Secretary, as appropriate, regarding implementation of measures or actions that will effectively address the identified threat.

"(3) APPLICATION OF EMERGENCY MEASURES.—An order for emergency actions or measures under this subsection may apply to—

"(A) the Electric Reliability Organization referred to in section 215,

"(B) a regional entity with respect to the United States operations of the Electric Reliability Organization,

"(C) the regional entity, or

"(D) any owner, user, or operator of the bulk power system within the United States.

"(d) DISCONTINUANCE OF INTERIM MEASURES.—The Commission shall issue an order discontinuing any

1 measures or actions ordered under subsection (b) upon the
2 earliest of the following:
3 "(1) When the President (either directly or
4 through the Secretary of Energy) issues a written
5 order or directive provided to the Commission to the
6 effect that the threat to the bulk power system that
7 requires such measures, or actions no longer exists.
8 "(2) When the Commission determines in writ-
9 ing that the ordered measures or actions are no
10 longer needed to address the identified threat.
11 "(3) When a reliability standard developed and
12 approved pursuant to section 215 is implemented to
13 address the identified threat.
14 "(4) One year after the issuance of an order
15 under subsections (b) unless the President (either
16 directly or through the Secretary) issues a deter-
17 mination affirming the continuing nature of the
18 threat. A determination issued under this paragraph
19 shall expire upon the implementation of a standard
20 under section 215 to address the identified threat.
21 The Commission shall issue such order to be effective
22 within 30 days of the relevant triggering event set out in
23 paragraphs (1) through (4).
24 "(e) DISCONTINUANCE OF EMERGENCY MEAS-
25 URES.—The Commission shall issue an order dis-

1 continuing any measures or actions ordered under sub-
2 section (c) upon the earliest of the following:
3 "(1) When the President (either directly or
4 through the Secretary of Energy) issues a written
5 order or directive provided to the Commission to the
6 effect that the threat to the bulk power system that
7 requires such measures, or actions no longer exists.
8 "(2) When the Commission determines in writ-
9 ing that the ordered measures or actions are no
10 longer needed to address the identified threat.
11 "(3) When a reliability standard developed and
12 approved pursuant to section 215 is implemented to
13 address the identified threat.
14 "(4) With respect to orders under subsection
15 (c), one year after the issuance of an order unless
16 the President (either directly or through the Sec-
17 retary) issues a determination reaffirming the con-
18 tinuing nature of the threat. A determination issued
19 under this paragraph shall expire upon the imple-
20 mentation of a standard under section 215 to ad-
21 dress the identified threat.
22 The Commission shall issue such order to be effective
23 within 30 days of the relevant triggering event set out in
24 paragraphs (1) through (4).

"(f) PROTECTION OF UNCLASSIFIED SENSITIVE CYBERSECURITY INFORMATION.—

"(1) CONFIDENTIALITY PROCEDURES.—After notice and opportunity for comment, the Commission shall promulgate rules and procedures to prohibit the unauthorized disclosure of unclassified sensitive cybersecurity information—

"(A) which was developed or used in connection with the implementation of this section,

"(B) which specifically discusses cybersecurity threats, vulnerabilities, mitigation plans or security procedures, and

"(C) the unauthorized disclosure of which could be used in a malicious manner to impair the reliability or operations of the bulk power system or the supply of electricity to the bulk power system.

Such rules and procedures shall require the inventory and safeguarding of such information during its creation, storage and transmittal by the Commission or by any other entity, including any vendor, contractor or consultant.

"(2) LIMITED DISCLOSURE TO ENTITIES SUBJECT TO COMMISSION ACTION.—In the rules and procedures promulgated under paragraph (1), the

1 Commission shall authorize the release of sensitive
2 cybersecurity information to entities subject to Com-
3 mission action under this section and to their em-
4 ployees, contractors and third-party representatives,
5 to the extent necessary to enable such entities to im-
6 plement Commission rules, orders or measures. En-
7 tities originating, receiving or possessing such infor-
8 mation shall comply with Commission rules and pro-
9 cedures to limit disclosure of such information to
10 any other entities that have been determined to have
11 a need to know, have executed non disclosure agree-
12 ments, and have been deemed by the entity to be
13 trustworthy and reliable. Any entity which signed
14 such non disclosure agreement and was found by the
15 Commission or by another entity subject to this sec-
16 tion to have improperly disclosed sensitive cybersecu-
17 rity information shall thereafter be denied access to
18 such information, and the Commission shall suspend
19 ability of the entity disclosing such information to
20 appear before the Commission. The sanctions under
21 this paragraph against any individual or other entity
22 shall be in addition to, and not in lieu of, any other
23 actions Commission is authorized to take pursuant
24 to section 316A for failure to comply with the rules
25 or procedures established by the Commission under

1 this section. Information designated sensitive cyber-
2 security information pursuant to this section shall
3 not be subject to disclosure under the Freedom of
4 Information Act (5 U.S.C. 552).
5 "(3) LIMITATIONS.—
6 "(A) The Commission shall consult with
7 national security or national intelligence agen-
8 cies, as appropriate, for purposes of designating
9 certain information as sensitive cybersecurity
10 information, but shall not designate as sensitive
11 cybersecurity information any information that
12 has been classified by another Federal agency.
13 "(B) Nothing in this section shall be con-
14 strued to authorize the withholding of informa-
15 tion from the committees of the Congress with
16 jurisdiction over the Commission or the Comp-
17 troller General.
18 "(C) In promulgating and implementing
19 rules and procedures under this section, the
20 Commission shall protect from disclosure only
21 the minimum amount of sensitive cybersecurity
22 information necessary to protect the reliability
23 or operations of the bulk power system or the
24 supply of electricity to the bulk power system.
25 The Commission shall segregate sensitive cyber-

1 security information within documents, elec-
2 tronic communications, and rules, orders or
3 records associated with such rules and orders,
4 wherever feasible, to facilitate disclosure of in-
5 formation which is not designated as sensitive
6 cybersecurity information.

7 "(D) Information may not be designated
8 as sensitive cybersecurity information for longer
9 than 10 years, unless specifically redesignated
10 by the Commission.

11 "(E) The Commission is authorized to re-
12 move the designation of sensitive cybersecurity
13 information, in whole or in part, from a docu-
14 ment or electronic communication if the unau-
15 thorized disclosure could not be used to impair
16 the reliability or operations of the bulk power
17 system or the supply of electricity to the bulk
18 power system.

19 "(4) CONSISTENCY OF MARKINGS.—The Com-
20 mission is authorized to place markings on docu-
21 ments, in whole or in part, which designate the de-
22 gree of sensitivity and limitations on dissemination.
23 Regulations and related procedures may be modified,
24 as appropriate, to ensure consistency with applicable

1 Executive Orders or laws pertaining to controlled
2 unclassified information.
3 "(5) NONDISCLOSURE OF SENSITIVE CYBERSE-
4 CURITY INFORMATION IN RULES OR ORDERS.—If a
5 rule or order issued pursuant to this section contains
6 sensitive cybersecurity information or if information
7 in the record associated with such rule or order con-
8 stitutes sensitive cybersecurity information, the
9 Commission may make the rule, order or informa-
10 tion non-public in whole or in part. The Commission
11 may disclose such non-public rule, order or informa-
12 tion to entities other than the recipient of the rule
13 or order, as the Commission deems necessary, to
14 carry out the rule or order and protect the reliability
15 of the bulk power system.
16 "(6) JUDICIAL REVIEW OF DESIGNATIONS.—
17 Any determination by the Commission concerning
18 the designation of sensitive cybersecurity informa-
19 tion shall be subject to judicial review pursuant to
20 subsection (a)(4)(B) of section 552 of title 5 of the
21 United States Code.
22 "(g) REVIEW.—The Commission shall act expedi-
23 tiously to resolve all applications for rehearing of orders
24 issued pursuant to this section which are filed under sec-
25 tion 313(a). Any person or other entity seeking judicial

1 review pursuant to section 313 may obtain such review
2 only in the United States Court of Appeals for the District
3 of Columbia Circuit. In the case of any petition for review
4 involving rules or orders containing or relating to security-
5 sensitive information, the Commission and parties shall
6 develop with the court appropriate measures to ensure the
7 confidentiality of such information, including, but not lim-
8 ited to, court filings under seal or otherwise in non-public
9 form, or judicial review in camera.

10 "(h) ENFORCEMENT DISCRETION.—The Commission
11 is authorized to impose penalties pursuant to section 316A
12 for any violation of a rule or order of the Commission
13 under this section. The Commission shall exercise its dis-
14 cretion in engaging in enforcement actions under this sec-
15 tion to recognize good faith efforts to comply with direc-
16 tives of the Commission.

17 "(i) PAPERWORK REDUCTION.—Chapter 35 of title
18 44, United States Code (44 U.S.C. 3501 et seq.) (com-
19 monly referred to as the 'Paperwork Reduction Act') shall
20 not apply to collections of information that relate to meas-
21 ures or actions described in this section.

22 "(j) PROVISION OF ASSISTANCE TO INDUSTRY IN
23 MEETING CYBERSECURITY PROTECTION NEEDS.—

24 "(1) EXPERTISE AND RESOURCES.—The Sec-
25 retary shall establish a program to develop expertise

1 and identify technical and electronic resources, in-
2 cluding hardware, software and system equipment,
3 helpful to cybersecurity protection of the electric
4 grid and all electric systems, including distribution-
5 level electric systems.

6 "(2) SHARING EXPERTISE.—The Secretary
7 shall offer to share such expertise through consulta-
8 tion and assistance with any owner, operator, or
9 user of the bulk power system, to any owner or oper-
10 ator of an electricity distribution system located in
11 the United States whether or not connected to the
12 bulk power system, and specifically to any owner or
13 operator of an electricity distribution system that
14 may provide electricity to national defense and other
15 critical-infrastructure facilities of the United States.

16 "(3) PRIORITY.—The Secretary shall consult
17 with the Commission, the Secretary of Defense, the
18 Secretary of Homeland Security, and other Federal
19 agencies to confirm the identity of States and elec-
20 tric systems serving such national defense and crit-
21 ical-infrastructure facilities, and shall assign higher
22 priority to such States and systems in offering such
23 support.

24 "(4) CLEARANCES.—The Secretary shall facili-
25 tate the acquisition by key security personnel of any

electric entity affected by this subsection of sufficient security clearances to allow such personnel access to information that would enable optimum understanding of cybersecurity threats and ability to respond.

"(5) DEFENSE FACILITIES.—Within one year of the date of enactment of this section, the States of Alaska and Hawaii and the Territory of Guam shall prepare, in consultation with the Secretary of Energy, the Secretary of Defense, and the electric utilities that serve national defense facilities in those jurisdictions, a comprehensive plan, to be implemented by the relevant State and territorial governmental authorities, identifying the emergency measures or actions that will be taken to protect the reliability of the electric power supply of the national defense facilities located in those jurisdictions in the event of an imminent cybersecurity threat. A copy of each such plan shall be provided to the Secretary of Energy and the Secretary of Defense.".

(b) CONFORMING AMENDMENT.—Section 201(b)(2) of the Federal Power Act is amended by inserting "215A" after "215".

○

AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

I

111TH CONGRESS
1ST SESSION

H. R. 2195

To amend the Federal Power Act to provide additional authorities to adequately protect the critical electric infrastructure against cyber attack, and for other purposes.

IN THE HOUSE OF REPRESENTATIVES

APRIL 30, 2009

Mr. THOMPSON of Mississippi (for himself, Mr. KING of New York, Ms. CLARKE, Mr. DANIEL E. LUNGREN of California, Ms. JACKSON-LEE of Texas, Ms. LORETTA SANCHEZ of California, Ms. HARMAN, Mr. CUELLAR, Mr. CARNEY, Ms. ZOE LOFGREN of California, Mr. PASCRELL, Mr. LUJÁN, and Mr. LANGEVIN) introduced the following bill; which was referred to the Committee on Energy and Commerce, and in addition to the Committee on Homeland Security, for a period to be subsequently determined by the Speaker, in each case for consideration of such provisions as fall within the jurisdiction of the committee concerned

---

A BILL

To amend the Federal Power Act to provide additional authorities to adequately protect the critical electric infrastructure against cyber attack, and for other purposes.

1 *Be it enacted by the Senate and House of Representa-*
2 *tives of the United States of America in Congress assembled,*

3 **SECTION 1. CRITICAL ELECTRIC INFRASTRUCTURE.**

4 (a) FINDINGS.—

5 (1) The critical electric infrastructure of the
6 United States and Canada has more than $1 trillion

in asset value, more than 200,000 miles of transmission lines, and more than 800,000 megawatts of generating capability, serving over 300 million people.

(2) The effective functioning of this infrastructure is highly dependent on computer-based control systems that are used to monitor and manage sensitive processes and physical functions.

(3) These control systems are becoming increasingly connected to open networks, such as corporate intranets and the Internet. According to the Department of Homeland Security's United States Computer Emergency Readiness Team ("US–CERT"), this transition towards widely used technologies and open connectivity exposes control systems to the ever-present cyber risks that exist in the information technology world in addition to control system specific risks.

(4) Malicious actors pose a significant risk to this infrastructure. The Federal Bureau of Investigation ("FBI") has identified multiple sources of threats, including foreign nation states, domestic criminals and hackers, and disgruntled employees.

(5) Intentional or naturally occurring Electromagnetic Pulse ("EMP") events also threaten crit-

ical electric infrastructure. The Commission to Assess the Threat to the United States from EMP Attack reported in 2008 that an EMP attack could cause significant damage or disruption to critical electric infrastructure and other critical infrastructure due to the widespread use of Supervisory Control and Data Acquisition ("SCADA") systems. The National Academy of Sciences also reported in 2008 that Severe Space Weather Events could produce similar results.

(6) The Department of Homeland Security's Control Systems Security Program is designed to increase the reliability, security, and resilience of control systems to guard against and enhance domestic preparedness for and collective response to a cyber attack by a terrorist or other person. This is done by developing voluntary cyber risk reduction products, supporting the Department of Homeland Security's Industrial Control Systems Computer Emergency Response Team ("ICS–CERT") in developing vulnerability mitigation recommendations and strategies, and coordinating and leveraging activities for improving the Nation's critical infrastructure security posture.

1 (7) According to recent news reports, the elec-
2 tronic control systems of the electrical system in the
3 United States have been routinely penetrated and
4 compromised. According to current and former na-
5 tional security officials, cyber spies from China, Rus-
6 sia, and other countries have penetrated the United
7 States electrical system in order to map the system,
8 and have left behind software programs that could
9 be used to disrupt and disable the system.
10 (8) In the interest of national security, and to
11 enhance domestic preparedness for and collective re-
12 sponse to a cyber attack by a terrorist or other per-
13 son, a statutory mechanism is necessary to protect
14 the critical electric infrastructure against cyber
15 threats.
16 (9) In spite of existing mandatory cybersecurity
17 standards, a report from the North American Elec-
18 tric Reliability Corporation ("NERC") suggests that
19 many utilities are underreporting their assets, poten-
20 tially to avoid compliance requirements. In April
21 2009, NERC reported that only 23 percent of re-
22 sponding utilities identified a "Critical Cyber Asset"
23 as required by NERC Reliability Standard 002–1.
24 According to NERC, the results of this survey sug-
25 gest that utilities may not have identified certain

1 qualifying assets as "Critical". NERC requested
2 that entities take a fresh, comprehensive look at
3 their methodology in order to identify and secure
4 more Critical Cyber Assets.

5 (10) On May 21, 2008, in testimony before the
6 House Committee on Homeland Security, Joseph
7 Kelliher, then-Chairman of the Federal Energy Reg-
8 ulatory Commission ("the Commission"), stated that
9 his agency is in need of additional legal authorities
10 to adequately protect the electric power system
11 against cyber attack.

12 (b) RESEARCH ON CYBER COMPROMISE OF CRITICAL
13 ELECTRIC INFRASTRUCTURE.—(1) Pursuant to section
14 201 of the Homeland Security Act of 2002 (6 U.S.C. 121)
15 and in furtherance of domestic preparedness for and col-
16 lective response to a cyber attack by a terrorist or other
17 person, the Secretary of Homeland Security, working with
18 other national security and intelligence agencies, shall con-
19 duct research and determine if the security of federally
20 owned programmable electronic devices and communica-
21 tion networks (including hardware, software, and data) es-
22 sential to the reliable operation of critical electric infra-
23 structure have been compromised.

24 (2) The scope of the research referred to in para-
25 graph (1) shall include: the extent of compromise, identi-

1 fication of attackers, the method of penetration, ramifica-
2 tions of the compromise on future operations of critical
3 electric infrastructure, secondary ramifications of the com-
4 promise on other critical infrastructure sectors and the
5 functioning of civil society, ramifications of compromise
6 on national security, including war fighting capability, and
7 recommended mitigation activities.

8 (3) The Secretary of Homeland Security shall report
9 the findings to the appropriate committees of Congress,
10 including the Committee on Homeland Security of the
11 House of Representatives and the Homeland Security and
12 Governmental Affairs Committee of the Senate. The re-
13 port may contain a classified annex.

14 (c) FEDERAL POWER ACT AMENDMENT.—Part II of
15 the Federal Power Act (16 U.S.C. 791a and following)
16 is amended by adding the following new sections at the
17 end thereof:

18 **"SEC. 224 CRITICAL INFRASTRUCTURE.**

19 "(a) DEFINITIONS.—For purposes of this section:

20 "(1) CRITICAL ELECTRIC INFRASTRUCTURE.—
21 The term 'critical electric infrastructure' means sys-
22 tems and assets, whether physical or cyber used for
23 the generation, transmission, distribution, or meter-
24 ing of electric energy that, in the determination of
25 the Commission, in consultation with the Secretary

of Homeland Security and other national security agencies, are so vital to the United States that the incapacity or destruction of such systems and assets, either alone or in combination with the failure of other assets, would cause significant harm to the security, national or regional economic security, or national or regional public health or safety.

"(2) CRITICAL ELECTRIC INFRASTRUCTURE INFORMATION.—The term 'critical electric infrastructure information' means critical infrastructure information related to critical electric infrastructure.

"(3) CRITICAL INFRASTRUCTURE INFORMATION.—The term 'critical infrastructure information' has the same meaning as is given that term in section 212(3) of the Critical Infrastructure Information Act of 2002 (6 U.S.C. 131(3)).

"(4) CYBER THREAT.—The term 'cyber threat' means any act by a terrorist or other person that disrupts, attempts to disrupt, or poses a significant risk of disruption to the operation of programmable electronic devices and communication networks (including hardware, software, and data) essential to the reliable operation of critical electric infrastructure.

1 "(5) CYBER VULNERABILITY.—The term 'cyber
2 vulnerability' means any weakness that, if exploited
3 by a terrorist or other person, poses a significant
4 risk of disruption to the operation of programmable
5 electronic devices and communication networks (in-
6 cluding hardware, software, and data) essential to
7 the reliable operation of critical electric infrastruc-
8 ture.
9 "(b) ASSESSMENT, REPORT, AND DETERMINA-
10 TION.—
11 "(1) IN GENERAL.—Pursuant to section 201 of
12 the Homeland Security Act of 2002 (6 U.S.C. 121),
13 the Secretary of Homeland Security shall assess
14 cyber vulnerabilities or threats to critical infrastruc-
15 ture, including critical electric infrastructure and ad-
16 vanced metering infrastructure, on an ongoing basis
17 and produce reports, including recommendations, on
18 a periodic basis for the purposes of homeland secu-
19 rity, including the enhancement of domestic pre-
20 paredness for and collective response to a cyber at-
21 tack by a terrorist, nation-state, or other person,
22 and for other purposes.
23 "(2) ELEMENTS OF THE REPORT.—The Sec-
24 retary shall—

"(A) include in the reports under this section findings regarding a cyber vulnerability or terrorist threat or potential terrorist threat, and a nation-state threat or potential threat to critical electric infrastructure; and

"(B) provide recommendations regarding actions that may be performed to enhance individualized and collective domestic preparedness and response to the cyber vulnerability or terrorist or nation-state.

"(3) TRANSMITTAL OF REPORT.—The Secretary of Homeland Security shall transmit reports prepared in response to the cyber vulnerability or threat to the Commission and the appropriate committees of Congress, including the Committee on Homeland Security of the House of Representatives and the Homeland Security and Governmental Affairs Committee of the Senate, of the Secretary's determinations under this section. Each such report may contain a classified annex.

"(4) TIMELY DETERMINATION.—If, in carrying out the assessment required under paragraph (1), the Secretary of Homeland Security determines that a significant cyber vulnerability or threat to critical electric infrastructure has been identified, the Sec-

1 retary of Homeland Security shall communicate such
2 a determination to the Commission in a timely man-
3 ner. The Secretary of Homeland Security may incor-
4 porate intelligence or information received from
5 other national security or intelligence agencies in
6 making such determination.
7 "(c) COMMISSION AUTHORITY.—
8 "(1) ISSUANCE OF RULES OR ORDERS.—Fol-
9 lowing receipt of a finding under subsection (b), the
10 Commission shall issue (and from time to time
11 thereafter amend) such rules or orders as are nec-
12 essary to protect critical electric infrastructure
13 against vulnerabilities or threats.
14 "(2) EMERGENCY PROCEDURES.—The Commis-
15 sion may issue, in consultation with the Secretary of
16 Homeland Security, a rule or order under this sec-
17 tion without prior notice or hearing if it determines
18 the rule or order must be issued immediately to pro-
19 tect critical electric infrastructure from an imminent
20 threat or vulnerability.
21 "(d) DURATION OF EMERGENCY RULES OR OR-
22 DERS.—Any rule or order issued by the Commission with-
23 out prior notice or hearing under subsection (c)(2) shall
24 remain effective for not more than 90 days unless, during
25 such 90 days, the Commission gives interested persons an

1 opportunity to submit written data, views, or arguments
2 (with or without opportunity for oral presentation) and af-
3 firms, amends, or repeals the rule or order.

4 "(e) JURISDICTION.—Notwithstanding section 201,
5 the provisions of this section shall apply to any entity that
6 owns, controls, or operates critical electric infrastructure,
7 and such entities shall be subject to the jurisdiction of the
8 Commission for purposes of carrying out this section and
9 for purposes of applying the enforcement authorities of
10 this Act with respect to such provisions, but shall not
11 make an electric utility or any other entity subject to the
12 jurisdiction of the Commission for any other purposes.

13 "(f) PROTECTION OF CRITICAL ELECTRIC INFRA-
14 STRUCTURE INFORMATION.—The provisions of section
15 214 of the Homeland Security Act of 2002 (6 U.S.C. 133)
16 shall apply to critical electric infrastructure information
17 submitted to the Commission under this section to the
18 same extent that they apply to critical infrastructure in-
19 formation voluntarily submitted to the Department of
20 Homeland Security under that Act (6 U.S.C. 101 and fol-
21 lowing).

1 **"SEC. 224B. PROTECTION AGAINST KNOWN CYBER**
2 **VULNERABILITIES OR THREATS TO THE**
3 **CRITICAL ELECTRIC INFRASTRUCTURE.**

4 "(a) INTERIM MEASURES.—After notice and oppor-
5 tunity for comment, the Commission shall establish, in
6 consultation with the Secretary of Homeland Security, by
7 rule or order, within 120 days of enactment of this section,
8 such mandatory interim measures as are necessary to pro-
9 tect against known cyber vulnerabilities or threats to the
10 reliable operation of the critical electric infrastructure in
11 the United States. Such interim reliability measures:

12 "(1) shall serve to supplement, replace, or mod-
13 ify cybersecurity reliability standards that, as of the
14 date of enactment of this section, were in effect pur-
15 suant to section 215, but that are determined by the
16 Commission, in consultation with the Secretary of
17 Homeland Security and other national security agen-
18 cies, to be inadequate to address known cyber
19 vulnerabilities or threats; and

20 "(2) may be replaced by new cybersecurity reli-
21 ability standards that are developed and approved
22 pursuant to section 215 following the date of enact-
23 ment of this section.

24 "(b) PLANS.—The rule or order issued under this
25 subsection may require any owner, user or operator of crit-
26 ical electric infrastructure in the United States to develop

1 a plan to address cyber vulnerabilities or threats identified
2 by the Commission and to submit such plan to the Com-
3 mission for approval.".

4 **SEC. 2. EVALUATION OF EXISTING AUTHORITIES.**

5 Section 214 of title II, subtitle B of the Homeland
6 Security Act of 2002 (6 U.S.C. 133(i)) is amended by add-
7 ing at the end the following:

8 "(i) REVIEW OF AUTHORITIES TO PROTECT CRIT-
9 ICAL INFRASTRUCTURE.—The Secretary of Homeland Se-
10 curity shall evaluate the capacity and authority of the De-
11 partment of Homeland Security and other Federal agen-
12 cies to ensure the security and resilience of electronic de-
13 vices and communication networks essential to each of the
14 critical infrastructure sectors identified pursuant to
15 Homeland Security Presidential Directive 7 against a
16 cyber attack by a terrorist, nation-state, or other person,
17 for the purpose of enhancing domestic preparedness for,
18 and collective response to, a cyber attack by a terrorist,
19 nation-state, or other person and to enhance the Nation's
20 homeland security posture.".

○

Mr. MARKEY. I commend Mr. Barrow and Chairman Thompson for their leadership on this critical issue.

I think it is fair to say that the Barrow bill, of which I am a cosponsor, would establish the minimum new authority that all parties, including the utility industry and State regulators, agree is necessary. However, many parties argue persuasively that we must go further in order to adequately address the threats before us. I have kept an open mind on these issues, and I urge the other members of this subcommittee to do likewise.

I am committed to working closely with Mr. Upton and Mr. Barton, along with Mr. Barrow and Chairman Waxman and all the other members of the committee, to move strong grid security legislation as soon as possible. This hearing represents an important first step in that direction.

I thank the witnesses for joining us. I look forward to your testimony.

And now I turn and recognize the ranking member of the committee, Mr. Upton.

OPENING STATEMENT OF HON. FRED UPTON, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF MICHIGAN

Mr. UPTON. Well, thank you, Mr. Chairman. And I do want to thank you for holding this very important hearing. We appreciate our witnesses joining us this morning, as well.

The House Homeland Security Committee has examined this issue, focusing on the vulnerability in electric generator control systems which could allow remote access, enabling a bad actor to remotely destroy a generator. We have also begun to look at these issues here, including classified hearings with the Department of Defense and Homeland Security, FERC, and others just last week.

Today, we will seek additional answers, with a focus on the most productive way to ensure the security of our energy infrastructure. I know we can work together on bipartisan legislation to address this very, very serious issue.

It is my hope that legislation to protect our critical infrastructure will also include Alaska, Hawaii, and our territories. Currently, NERC does not cover those areas, and our critical national security assets, particularly in Alaska and Hawaii, are too important to ignore.

Domestic infrastructure should be protected for cybersecurity generally, in addition to physical and electromagnetic threats. Additionally, I don't think it is enough to just cover the bulk power system; we also must include the distribution system. It has become clear that the distribution system outages and vulnerabilities can lead to problems with the bulk power system, and critical defense facilities are connected at the distribution level.

There is no question that this legislation should be comprehensive. We should seek to fill as many security gaps as possible. The threats that we face are too serious and abundant to only address a small portion of our vulnerability. The stakes could not be higher.

And, as we know, security is not free. There will be a cost to protecting our critical energy and national defense infrastructure. Our legislation should provide a mechanism by which all generators, regardless of whether or not they are rate-regulated by a State PUC,

are capable of covering the cost of investments that they are required to make in the name of protecting the national security of the U.S.

The security of our Nation's energy infrastructure from attack is one of the most important issues that our committee will address. It is not an issue that we can take lightly or cover in just one hearing.

Energy has certainly been one of the leading issues debated in Congress this year, rightfully so. Energy literally powers our economy. Even small price spikes and supply disruptions can wreak havoc on the economy. It is imperative that the security of our Nation's energy infrastructure gets the attention it deserves.

I yield back.

Mr. MARKEY. The gentleman's time has expired.

The Chair recognizes the gentleman from Michigan, chairman emeritus of our committee, Mr. Dingell.

OPENING STATEMENT OF HON. JOHN D. DINGELL, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF MICHIGAN

Mr. DINGELL. Mr. Chairman, thank you. I commend you for holding this hearing today. The reliability of this Nation's electricity grid in the face of its vulnerabilities to cybersecurity attacks is a matter of the utmost interest and concern.

Mr. Chairman, I would note that the White House has indicated that there will be a significant effort on the part of the administration to address the renewal of the grid. Therefore, this hearing comes at a very important time because, in addition to addressing the questions of efficiency of the grid, we can also see to it that questions relative to the safety and security of the grid are also addressed.

If there were a successful remote cyber attack on a plant's utility control systems, we could face something more serious than a brief brownout or blackout. The Idaho National Laboratory has shown how a hacker can remotely turn a large generator into a smoldering scrap pile in just a few moments. Known as the "Aurora vulnerability," this type of attack could destroy generating equipment and impair the generation and delivery of electricity across the entire area of North America for weeks or months, its consequences cascading on consumers, on our economy, on our health care system, and on our national defense assets, amongst other things.

These concerns are not just theoretical. It has been reported that China, Russia, and other nations have conducted cyber probes of the U.S. grid systems. Moreover, cyber attacks have actually been conducted against critical infrastructure in other countries.

In response to the Department of Homeland Security's worrying about Aurora vulnerability, the North American Electric Reliability Corporation, NERC, issued an advisory in June 2007 which outlined immediate and longer-term mitigation measures for utilities. An FERC audit of 30 utilities found that, 2 years later, progress had been made but that very significant issues still remain.

As the Electricity Reliability Organization designated under Section 215 of the Energy Policy Act of 2005, NERC has developed reliability standards for critical infrastructure protection. However,

there are significant gaps, given the nature of a national security threat. We need to extend Federal authority to take emergency actions as necessary to protect the grid. I look forward to building a bipartisan consensus on legislation which will ensure that the Federal Government has all the necessary powers to intervene when there are emergencies that threaten the Nation's electricity supply.

I also welcome our panel of witnesses. It is my hope that they can inform us on whether emergency power should extend beyond the bulk power system to utility systems in Alaska, Hawaii, Guam, and in other American possessions or areas.

These powers should also be able to reach critical distribution systems in places like the District of Columbia or New York City. We want to be sure that the legislation addresses threats to the electrical system and that the Federal Government is not improperly hobbled by legal and jurisdictional boundaries in the case of emergencies.

Thank you, Mr. Chairman.

Mr. MARKEY. Great. The gentleman's time has expired.

The Chair recognizes the gentleman from Illinois, Mr. Shimkus.

OPENING STATEMENT OF HON. JOHN SHIMKUS, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF ILLINOIS

Mr. SHIMKUS. Thank you, Mr. Chairman.

I, too, concur that this is a very important meeting, and I appreciate you all coming to help us sort through this.

You know, I had recently retired, about a year ago, from the Army Reserves. I served 3 years actively in West Germany. And, throughout my years here, I have always followed up on comments about the electromagnetic pulse concern, whether from natural occurrences or ships or a nuclear burst.

And we have always talked about smart metering is like the Holy Grail of energy efficiency. I think some people would argue that we set ourselves more at risk on some of this if it is an intentional electromagnetic burst in the atmosphere because of the ability to fry out this smart metering in all these solid-state applications, and the recovery time would be much greater than if we kept it simple.

So that will be my focus to debate, to hear, to try to figure out what is good and how far should we go, but, again, being careful that we don't try to automate so much that we actually decrease our ability to have a quick recovery, whether there be an intentional electromagnetic pulse burst or something that will naturally occur that will cause us great harm.

It was interesting, I heard a story out of St. Louis. I live close to St. Louis, Missouri. The nuclear power plant in Missouri is still on dial-up for its communications, just dial-up communications. And one of the things that they mentioned was, well, they don't really want to be on broadband because they don't want cybersecurity issues, they don't want some other types of concerns.

So it will be interesting to follow—again, this is all just basically over-the-radio broadcast news, so I look forward to following that up.

Thank you, Mr. Chairman. I yield back.

Mr. MARKEY. Great. The gentleman's time has expired.

The Chair recognizes the gentlelady from California, Ms. Matsui.

OPENING STATEMENT OF HON. DORIS O. MATSUI, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF CALIFORNIA

Ms. MATSUI. Thank you, Mr. Chairman, and thank you for calling this hearing. I am very pleased to be here today and would just take a couple minutes so we can continue on to the distinguished witnesses.

I would like to thank today's panelists for joining us to discuss the security of our electric grid, with regard to the two pending pieces of legislation. In particular, I would like to welcome my friend and constituent, John DiStasio, general manager and CEO of Sacramento Municipal Utility District, otherwise known as SMUD, to today's hearing.

John has served SMUD most admirably for nearly 30 years. He originally joined the utility as a buyer for the district's purchasing department. He was promoted to the utility's top post last year, after serving as the assistant general manager since 2000 and being awarded a number of customer service honors.

I look forward to hearing his views on ways in which we can legislatively address cybersecurity issues in relation to protecting our electric infrastructure.

Additionally, I look forward to hearing all of your expert opinions. The expertise you share here will be useful throughout the committee process and in considering these measures.

As we are aware, the world has become critically reliant on digital communications, making military targets, civilian infrastructure, particularly our electric grid, vulnerable to cyber attack. The electric grid is a significant part of our country's infrastructure. Failure to take preventative steps to ensure its protection significantly endangers our economy.

It is critical that we examine the existing regulatory authorities that respond to threats aimed at our power system. And we need to continually examine the expanding risk of cyber attacks and the implications for traditional methods of deterrence. This committee is well-positioned to examine this issue and has already suggested one manner in which to address it. Together, we can ensure that we have the tools and resources necessary to effectively defend our electric infrastructure.

I look forward to hearing from the panelists on the bills before us today and working with the committee and stakeholders on these important matters. Once again, I thank you, Mr. Chairman, for highlighting this important topic. And I yield back the balance of my time.

Mr. MARKEY. The gentlelady's time has expired.

The Chair recognizes the gentleman from Florida, Mr. Stearns.

OPENING STATEMENT OF HON. CLIFF STEARNS, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF FLORIDA

Mr. STEARNS. Good morning. And thank you, Mr. Chairman, and thank the ranking member, Mr. Upton, for calling this really important hearing, which basically is addressing the vulnerability of

the Nation's electrical grid to cyber attacks and the steps that are needed to be taken to protect this critical infrastructure.

It has become apparent, I think, to all that our electric grid is vulnerable to cyber attacks by terrorists and by other nations. Our Nation's infrastructure systems are heavily, obviously, reliant on computer-based systems that are used to monitor and control sensitive processes and physical functions. These systems were once mostly closed proprietary operations but are increasingly connecting to open networks, like corporate intranets and the Internet.

The transition towards widely used technologies and open connectivity exposes the control system to the ever-present cyber risks that exist in the information technology world in addition to control-system-specific tasks.

Driving such concerns are reports that malicious attacks are rising on specialized computer control systems that open and shut valves on natural gas pipelines, throw circuit breakers on power lines, and make telecommunications and defense networks, nuclear power plants, and hydro dams do their jobs.

To address these vulnerabilities, the Institute for Human and Machine Cognition, which is part of the Florida Institute of Technology and partnership thereof—Mr. Chairman, it is located in my hometown of Ocala, Florida—is creating new processes for better defending supervisory control and data acquisition systems, SCADA, from attack. Such systems, known as SCADA, monitor and report on the functions of closed computerized networks that provide real-time data in the operation of these central facilities.

For example, SCADA networks could track something as simple as a climate control system in an office building or monitor the key workings of something as complex and expansive as a nuclear power plant. SCADA networks are also widely used to control the flow of oil and natural gas through pipelines, dams, and many non-energy-related processes such as water and sewer lines, telecommunication systems, and mass transit systems.

So, Mr. Chairman, I think this is a very good hearing, and I look forward to our witnesses.

Mr. MARKEY. Great. The gentleman's time has expired.

The Chair recognizes the gentleman from California, Mr. McNerney.

OPENING STATEMENT OF HON. JERRY MCNERNEY, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF CALIFORNIA

Mr. MCNERNEY. Well, I want to thank you, Mr. Chairman, for calling this meeting on the critical issue that is in front of us and also a very fascinating issue.

I want to thank the witnesses. I have looked at your resumes, and I am very pleased with the caliber of information you are going to bring in front of us.

Mr. DiStasio, from my area in California, I appreciate your coming out here today.

It amazes me that we have a network, a physical network, of electrical system that serves our country that is vulnerable to cyber attack that can bring down large portions of our country. So the question is, what do we do about it? And we need to worry both

about how to prevent attacks, how to make ourselves less vulnerable, and also how to plan for contingencies if attacks are successfully carried out, both cyber and physical attacks.

So these are big issues. The issue is complicated, but we look forward to getting some concrete ideas from you.

I want to thank Mr. Barrow for your leadership on this; Bennie Thompson, who is not here, for his leadership. This is what we need, this kind of forward-looking leadership.

So thank you all for coming, and I look forward to your testimony.

Mr. MARKEY. The gentleman's time has expired.

The gentlelady from Wisconsin, Ms. Baldwin, is recognized.

OPENING STATEMENT OF HON. TAMMY BALDWIN, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF WISCONSIN

Ms. BALDWIN. Thank you, Mr. Chairman, for holding this important hearing on protecting the Nation's electric grid from cyber attacks and other threats.

The threat of someone with ill intent attacking and accessing the control systems of electric generators or other equipment presents a substantial concern that must be addressed. These cyber or other forms of attacks, perpetrated with the intent to disrupt services in the short term or wreak long-term havoc by damaging equipment, could have a significant impact not only on our national security but also our economic security. In fact, according to one estimate, if a third of the country lost power for 3 months, the economic price tag would be $700 billion.

The Idaho National Laboratory test, known as Aurora, which has been cited a couple of times already, demonstrated how an attacker could break into a control system and disrupt the grid. This test highlighted the seriousness of a potential threat to our infrastructure and the urgency with which Congress and our Nation's agencies must act to mitigate any consequences.

As we consider the two bills before us, we must remember that we have a responsibility to remain vigilant, to make sure that our agencies have the proper tools to protect against cyber attacks, and to ensure that industry is fully prepared to work in concert with government to prevent any disruptions.

I look forward to hearing from our witnesses today about how we can best address these reliability and security issues.

Thank you, Mr. Chairman. I yield back the balance of my time.

Mr. MARKEY. The gentlelady's time has expired.

The gentleman from Georgia, the sponsor of this legislation, who I would like to congratulate for his excellent efforts in this area, is recognized for 2 minutes.

OPENING STATEMENT OF HON. JOHN BARROW, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF GEORGIA

Mr. BARROW. Well, thank you, Mr. Chairman. And thank you for moving this legislation forward and for the opportunity to work together on this issue of critical importance to our homeland security.

I am a sponsor of H.R. 2165, the "Bulk Power System Protection Act of 2009," one of the subjects of today's hearing, because I am

convinced that the threats to our critical energy infrastructure are every bit as real and every bit as dangerous as any threat we can imagine. I am pleased that this Congress and this committee have given this a high priority and will push forward to pass meaningful legislation.

I obviously think that my bill is on the right track, but I am open to new angles, incorporating new ideas into the mix. I encourage my colleagues to cosponsor H.R. 2165, and let's use it as a foundation for working together on these solutions.

The key to sustainable security is that government and industry identify and address evolving threats against our country together. As our society becomes more and more reliant on technological advances, we actually become more and more vulnerable to debilitating attacks. This hearing is an important first step toward closing security gaps which threaten us. The time to act is now; the American people expect it, and our national security demands it.

I thank the witnesses for being here today, and I thank the chairman for the time. And I yield back the balance of my time.

Mr. MARKEY. I thank the gentleman for his work.

All time for opening statements has been completed.

Chairman Bennie Thompson, chairman of the Homeland Security Committee and lead sponsor of H.R. 2195, one of the bills that we are considering today, has submitted a written statement for the record. I would like unanimous consent that that statement be entered into the record.

Without objection, so ordered.

[The prepared statement of Mr. Thompson follows:]

Statement for the Record
Chairman Bennie G. Thompson
U.S. House of Representatives Committee on Homeland Security

Hearing before the House Committee on Energy and Commerce
Subcommittee on Energy and Environment
October 27, 2009

I. Introduction and Overview

Good morning. I'd like to begin by thanking Chairman Markey for allowing me to submit a written statement on this critical issue of national security. I very much appreciate his interest in the subject of cybersecurity as it relates to the electric grid, and I commend him, Chairman Waxman, and the staff for their efforts in this area.

As Chairman of the Committee on Homeland Security (CHS), I am extremely concerned about the security of our nation's electric grid. I want to clearly state that I believe America is disturbingly vulnerable to a cyber attack or other damaging geo-magnetically induced currents. Such incidents could cause significant consequences to our nation's critical infrastructure. Virtually every expert that I've discussed these matters with – across government and throughout the private sector – shares this assessment.

In just the past three years, the Committee on Homeland Security – principally through the Subcommittee on Emerging Threats, Cybersecurity, Science and Technology – has held eleven hearings and conducted dozens of investigations on cybersecurity vulnerabilities. During this time, the Committee conducted a review into the efforts of owners and operators of the bulk power system ("BPS") to secure their information networks. Committee members became concerned about the adequacy of the North American Electric Reliability Corporation ("NERC") critical infrastructure protection standards – the industry's self-created standards that require owners and operators to secure their electric equipment. Our Members, on a bipartisan basis, do not believe that they provide the appropriate amount of protection that the American people expect.

In testimony before the Subcommittee on Emerging Threats, Cybersecurity, Science and Technology on May 21, 2008, then-Chairman Joseph Kelliher of the Federal Energy Regulatory Commission ("the Commission") stated that his agency is in need of additional legal authorities to adequately protect the BPS against cyber attack. After extensive review and consideration of Federal and State policies regarding the reliability of the U.S. electric system, many of my colleagues and I concluded that existing efforts to protect the BPS also fall short of protecting other critical electrical assets, including transmission, distribution, and metering systems. Therefore, on April 30, 2009, together with Ranking Member Peter King and eleven other CHS Members, I introduced H.R. 2195, the "Critical Electric Infrastructure Protection Act," which creates a different scope of protected assets known as critical electric infrastructure ("CEI"). This type of infrastructure includes generation, transmission, distribution, and metering assets. To date, there are 26 bipartisan co-sponsors on H.R. 2195 and companion legislation has been introduced by Senator Joe Lieberman of the Senate Committee on Homeland Security and Governmental Affairs.

H.R. 2195 will grant authority to FERC, working with other national security agencies, to issue emergency orders to owners and operators of generation, transmission, distribution, and metering systems in the event of an imminent cyber attack or electromagnetic pulse. This legislation will also require FERC to establish interim measures deemed necessary to protect against known cyber threats to critical electric infrastructure, which may supplement or replace existing inadequate standards. H.R. 2195 also directs the Secretary of Homeland Security to investigate whether the security of Federally-owned critical electric infrastructure has been compromised by outsiders.

I believe that enactment of this homeland security legislation is necessary to secure our nation's most critical infrastructure. I thank the Committee for considering my bill and I look forward to working with you all in a bipartisan basis going forward.

II. Background: Threats and Vulnerabilities to the Electric System

The BPS of the United States and Canada has more than $1 trillion in asset value, more than 200,000 miles of transmission lines, and more than 800,000 megawatts of generating capability, serving over 300 million people.[1] The effective functioning of this infrastructure – and the CEI at large – is highly dependent on control systems, computer-based systems that are used to monitor and control sensitive processes and physical functions. Once largely proprietary and closed, control systems are becoming increasingly connected to open networks, such as corporate intranets and the Internet. As a result, according to the United States Computer Emergency Readiness Team ("US-CERT"), "this transition towards widely used technologies and open connectivity exposes control systems to the ever-present cyber risks that exist in the information technology world in addition to control system specific risks."[2]

Clearly, the risk to these systems is steadily increasing. Ten years ago, the President's Commission on Critical Infrastructure Protection ("PCCIP") released a report on the risks associated with interconnected computer systems on the CEI, stating that "the widespread and increasing use of supervisory control and data acquisition systems for control of energy systems provides increasing ability to cause serious damage and disruption by cyber means."[3] Since the release of that study, numerous unintentional cyber incidents – from the Davis-Besse power plant incident in 2003, to the Northeast blackout, to the Browns Ferry nuclear power plant failure in 2006 – suggest that the concerns raised by the PCCIP were warranted. Malicious actors also pose a significant risk to this infrastructure. The Federal Bureau of Investigation has identified multiple sources of threats, including foreign nation states, domestic criminals and hackers, and disgruntled employees working within an organization.[4]

---

[1] U.S. Government Accountability Office, Report to Congressional Requesters, *Critical Infrastructure Protection: Multiple Efforts to Secure Control Systems Are Under Way, but Challenges Remain* (October 2007), p. 27.
[2] U.S. Department of Homeland Security, Control System Security Program Fact Sheet, available at http://www.us-cert.gov/control_systems/pdf/CSSP_FactSheet_sml.pdf.
[3] U.S. Government Accountability Office, Report to Congressional Requesters, *Critical Infrastructure Protection: Challenges and Efforts to Secure Control Systems* (March 2004), p. 2.
[4] U.S. Government Accountability Office, Report to Congressional Requesters, *TVA Needs to Address Weaknesses in Control Systems and Networks* (April 2008), p. 8.

There are numerous public examples of threats and vulnerabilities that have had a negative and dangerous impact on electric systems and our homeland security. The potential consequences of an attack on control systems vary widely from the introduction of raw sewage into potable water systems[5] to the catastrophic failure of critical electrical generators due to the change of a single line of code in a critical system.[6] For example:

- Computers at an inactive nuclear power plant in Ohio were infected by the Slammer worm in January 2003.[7]
- Multiple criminal extortion schemes have exploited the use of control systems for economic gain.[8]
- There is evidence that al Qaeda is interested in the vulnerabilities of the U.S. public and private utilities.[9]
- The discovery in Afghanistan of a computer containing structural analysis programs for dams, combined with an increase in Web traffic relating to SCADA systems, prompted the National Infrastructure Protection Center ("NIPC") to issue a warning information bulletin.[10]
- Nation state adversaries have suggested that attacking our domestic critical infrastructure will be part of their war plans in an engagement with the United States. In a book endorsed by top Chinese People's Liberation Army leadership called "Unrestricted Warfare," two colonels describe using network attacks "to disrupt the civilian electricity network, traffic dispatching network, financial transaction network, and telephone communications networks," causing social panic and undermining political leadership.[11]

---

[5] U.S. Government Accountability Office, Report to Congressional Requesters, *Challenges and Efforts to Secure Control Systems* (2004) p. 17.
[6] Briefing by NCSD, INL to the Homeland Security Committee, March 15, 2007.
[7] Congressional Research Service "Critical Infrastructure: Control Systems and the Terrorist Threat," RL31534, p. 17.
[8] Infoworld, "Government cybersecurity gets an 'F,'" Sep. 11, 2006, available at http://www.infoworld.com/article/06/09/11/37NMmain_1.html.
[9] U.S. Government Accountability Office, Report to Congressional Requesters, *Challenges and Efforts to Secure Control Systems* (2004) p. 17.
[10] CRS Report RL31534, p. 7.
[11] Qiao Liang and Wang Xiangsui "Unrestricted Warfare," February 1999.

- According to recent news reports (Wall Street Journal, National Journal), the critical electric infrastructure of has been penetrated by spies from China, Russia, and other countries.[12]

Clearly, intentional and unintentional control system failures on the critical electric infrastructure can have a significant and potentially devastating impact on the economy, public health, and national security of the United States. For a society that runs on power, the discontinuity of electricity to chemical plants, banks, refineries, hospitals, and water systems presents a terrifying scenario. Economists recently suggested that the loss of power to a third of the country for three months would result in losses of over $700 billion.[13] This figure does not even take into account the potentially devastating societal or health ramifications that such an event could have on the American people.

An intentional or unintentional attack could also severely impact the ability of our war fighting capability. The Defense Science Board recently recognized the threat to critical Department of Defense ("DOD") military facilities that rely on the CEI. In a report titled "More Fight – Less Fuel" issued in February 2008, the Board concluded that "critical national security and homeland defense missions are at an unacceptably high risk of extended outage from failure of the grid and other critical national infrastructure."[14] The Board stated the grid "is highly vulnerable to prolonged outage from a variety of threats. This places critical mission assets at unacceptably high risk of extended disruption."[15] Furthermore, in the event of an attack on the CEI, the Board noted that the U.S. military cannot rely on on-site backup power generation:

> Although 99 percent of the electricity at U.S. military installations is from the commercial grid, backup power at installations is based on diesel

---

URL: http://www.terrorism.com/documents/unrestricted.pdf

[12] "Electric Grid in U.S. penetrated by spies," Wall Street Journal, April 8, 2009, available at http://online.wsj.com/article/SB123914805204099085.html

[13] (2007, Sept. 27). "Mouse click could plunge city into darkness, experts say," Retrieved Sept. 28, 2007, from http://www.cnn.com/2007/US/09/27/power.at.risk/index.html.

[14] Report of the Defense Science Board Task Force on DOD Energy Strategy, *More Fight – Less Fuel*, February 2008, available at http://www.acq.osd.mil/dsb/reports/2008-02-ESTF.pdf.

[15] Id., p. 53.

> generator sets with limited on-site fuel storage and not prioritized to critical tasks. As the reliability of the national grid has declined, the adequacy of backup power has become an issue. For both war fighting-related activity and the new Homeland defense mission, backup power is inadequate in terms of size, duration and reliability.[16]

The Board concluded that the DOD's approach to providing power to installations is based on assumptions that commercial power is highly reliable, subject to infrequent and short term outages, and backup can meet demands. Unfortunately, DOD's assumptions about commercial power and other critical infrastructure reliability are no longer valid and DOD must take a more rigorous risk-based approach to assuring adequate power to its critical missions. In the interest of national and homeland security, we must ensure effective and reliable energy flows to America's critical infrastructure facilities.

III. Homeland Security Committee Oversight

With these issues in mind, the Committee on Homeland Security's Subcommittee on Emerging Threats, Cybersecurity, Science and Technology initiated a review of the Federal government's effort and ability to ensure the security of the CEI from cyber attack. In October 2007, the Subcommittee held a hearing on the cyber threat to control systems, focusing particularly on a vulnerability to the CEI discovered by engineers at the Idaho National Laboratory. The vulnerability – known as "Aurora" – could enable a targeted attack on infrastructure connected to the electric grid, potentially destroying these machines and resulting in catastrophic losses of power for long periods of time. After engineers demonstrated a successful test of the vulnerability, the Department of Homeland Security ("DHS"), the Nuclear Regulatory Commission ("NRC") and the Commission began leading an effort to reach out to the private sector to mitigate the vulnerability.

[16] Id.

Under the framework of the Partnership for Critical Infrastructure Security,[17] DHS began its outreach efforts with the Electric and Nuclear sectors, which each identified a technical team and a set of subject matter experts to develop a mitigation strategy.[18] These two sectors began implementing the mitigations in varying degrees. On June 20, 2007, the Nuclear Sector issued a requirement for all members of their sector to implement short, medium, and long term mitigations for the vulnerability. On June 21, 2007, the Electric Sector (through the Electric Sector Information Sharing and Analysis Center, ES-ISAC) sent an advisory to its members with recommendations that they take similar action.

During the Subcommittee's October 2007 hearing, it became evident that the Nuclear Sector was well on its way toward implementing the mitigations; however, the extent to which Electric Sector companies were following the recommendations of the advisory was not clear. The difference in each sector's implementation stemmed from the cybersecurity regulatory requirements. In October 2007, the Commission had not yet adopted the Critical Infrastructure Protection reliability standards proposed by the North American Electric Reliability Corporation ("NERC"), which addressed cybersecurity requirements for the Electric Sector. Therefore, while the NRC could issue specific requirements for its owners and operators, the Electric Sector was unable to make similar demands.[19] CHS Members expressed concern during the hearing that these mitigation measures were not being fully implemented in the Electric Sector.

---

[17] The mission of the Partnership for Critical Infrastructure Security (PCIS) is to coordinate cross-sector initiatives that promote public and private efforts to help ensure secure, safe, and reliable critical infrastructure services.

[18] The Department held briefings at the FOUO level rather than classifying the information to the Secret level. The Department's justification for this was the importance of having the private sector aware and involved with mitigation of the vulnerability.

[19] Several things have changed since the Subcommittee hearing. On January 17, 2008, the Commission approved eight mandatory critical infrastructure protection reliability standards to protect the bulk power system against potential disruptions from cyber security breaches. These standards were developed by NERC, the private sector organization designated by the Commission as the electric reliability organization (ERO). These standards are currently in effect, though the industry has until approximately 2010 before they have to demonstrate "auditable compliance" with the standards. See NERC Revised Implementation Plan for Cybersecurity Standards.

These concerns were justified. Though NERC testified during the hearing that it sent a survey to industry members to determine compliance with the advisory and received a response from approximately 75 percent of the transmission grid that mitigations had been implemented or were in the process of being implemented,[20] the Committee later learned that the survey was not sent until October 19, 2007 – two days after the hearing.[21] Later, NERC staff suggested that they received information about the industry's mitigation efforts during a Critical Infrastructure Protection Committee meeting in St. Louis in September 2007. However, when the Committee asked participants about that meeting, none of the attendees were able to confirm that they discussed their mitigation efforts with NERC.

In light of these discrepancies, in mid-October 2007, the Emerging Threats Subcommittee, on a bipartisan basis, requested that Chairman Kelliher investigate the extent to which Electric Sector owners and operators implemented the mitigation efforts from the original Aurora advisory. Chairman Kelliher had expected to be able to draw upon results from NERC's October 19 industry survey; however, he determined that the survey lacked sufficient details of the mitigation efforts that would have provided the Commission with the certainty that the vulnerability had been addressed. For example, NERC's survey did not provide information about what facilities were the subject of the mitigation plans, what steps to mitigate the cyber vulnerability were being taken, and when those steps were planned to be taken – and, if certain actions were not being taken, why not. The Commission determined that it would have to undertake its own independent survey in order to obtain the information requested by the Homeland Security Committee.

The Commission continues to work with industry groups to informally gather information, on a voluntary basis, regarding the status of compliance with NERC's Aurora advisory. Initial observations suggested that while no company interviewed

---

[20] U.S. Congress, House Committee on Homeland Security, Hearing on "The Cyber Threat to Control Systems: Stronger Regulations are Necessary to Secure the Electric Grid," *testimony of David Whiteley*, 110th Cong., 1st sess., 17 Oct. 2007.
[21] Electric Sector ISAC (ESISAC) Advisory Follow-up Survey, Oct. 19, 2007.

ignored the advisory, compliance varied widely because there was a lack of baseline understanding of the threat and the application of the recommended mitigation measures among the utilities. This view is supported by the fact that all of the utilities interviewed requested additional information to help understand the technical implications of the attack and the specific strategies to mitigate the identified vulnerabilities. Through these selected interviews, the Commission has determined that although progress has been made by every entity that it interviewed, only a fraction of the owners and operators who responded appear to have performed all of the mitigations required by the Aurora advisory.

I, along with many of my colleagues, was deeply disturbed by the effectiveness of the Commission's efforts to address the Aurora threat. In response, I set out, together with Ranking Member King and the Emerging Threats Subcommittee to search out other means by which to ensure that the electric infrastructure (and the American populace that relies on its effective function) is better protected against these vulnerabilities. To that end, contemporaneous with a request for a Commission-led investigation, the Emerging Threats Subcommittee requested that the Commission assess its ability to respond to an imminent cyber attack under the current legal authorities contained in Section 215 of the Federal Power Act ("FPA"). We were concerned that the Commission not only lacked authority to regulate potentially vulnerable cybersecurity assets that are not covered in the promulgated standards,[22] but also the authority to issue orders to owners and operators in the event of an imminent exploitation of a BPS asset.

In testimony before the Subcommittee on May 21, 2008, then-Chairman Kelliher acknowledged for the first timeed that additional authorities are necessary to adequately protect the BPS against cyber attack. The Chairman noted that while Section 215 may

[22] The Homeland Security Committee has also argued that the NERC reliability standards are inadequate for protecting critical national infrastructure. For instance, telecommunications equipment is excluded from the standard's definition "critical cyber assets" list even though there are documented cases of computer worms denying service from control systems to substations. Ironically, some of these assets that could be exploited in an attack using the Aurora vulnerability are not considered "critical cyber assets." This means that if the Aurora vulnerability was discovered again tomorrow, NERC could not issue a "required action" to owners and operators under its jurisdiction because the "assets" affected by the Aurora vulnerability are not currently covered by CIP standards.

adequately protect the BPS against most reliability threats, the cybersecurity threat is different:

> [Cybersecurity] is a national security threat that may be posed by foreign nations, or others intent on undermining the U.S. through its electric grid. The nature of the threat stands in stark contrast to other major reliability vulnerabilities that have caused regional blackouts and reliability failures in the past, such as vegetation management and relay maintenance. Given the national security dimension to the cyber security threat, there may be a need to act quickly to protect the bulk power system, to act in a manner where action is mandatory rather than voluntary, and to protect certain information from public disclosure. Our legal authority is inadequate for such action.[23]

IV. Legislation

I believe that in the interest of national security, new statutory authority should be granted to FERC to protect the grid against cybersecurity threats. Specifically, I believe that the FPA should be amended to grant the Commission emergency authority to order temporary interim cybersecurity or other emergency standards when necessary to protect against a national security threat to the reliability of the BPS.

Further, to be truly effective, I believe it is necessary to go beyond the scope of the BPS, and include all assets that comprise CEI. The BPS is defined as the generation plants, the high voltage transmission system, and associated equipment, and does not normally include the distribution substations and lower voltage networks that distribute electricity to customers in a particular city or region. Alaska and Hawaii are specifically

[23] U.S. Congress, House Committee on Homeland Security, Hearing on "Implications of Cyber Vulnerabilities on the Resiliency and Security of the Electric Grid," *testimony of Joseph Kelliher*, 110th Cong., 2nd sess., 21 May 2008. Chairman Kelliher noted that "cyber vulnerabilities can require swift remedial action to protect the Nation's bulk power system," and that the standards development process can be "relatively slow." Furthermore, even though the Commission has an "Urgent Action" process, this can take one to three months to implement.

excluded from reliability regulations. In practice, many major cities and population centers are also excluded. This limitation leaves our nation vulnerable.

In January 2008, FERC approved the reliability standards developed by NERC to help safeguard the nation's BPS against potential disruptions from cyber attacks. The proposed standards require certain users, owners and operators of the grid to establish plans, protocols and controls to safeguard physical and electronic access to systems, to train personnel on security matters, to report security incidents, and to be prepared to recover information. By definition and design, the BPS Critical Infrastructure Protection Standards do not recognize the importance of continuity of electric power to chemical plants, banks, refineries, hospitals, water systems, and military installations, in and of themselves. Furhter, where they are located or their importance to society is not a factor in the determination of what parts of the greater U.S. electric system should be protected. This means that <u>any</u> Critical Infrastructure Protection Standard – including those recently approved by FERC – will focus on reliability of the BPS exclusively, and not on public health and safety or even economic stability from a "homeland security" perspective.

Prior to the September 11, 2001 attacks, a single-minded focus on BPS reliability against serendipitous hazards and accidents may have been defensible; but with the specter of terrorist or other bad actor attacking the electric grid to destabilize or harm our nation, preoccupation with the BPS <u>as a whole</u> falls short of the mark. For example, the reliable operability of a small substation powering a major oil or gas pipeline in a remote region is not important to the stability of the BPS grid, but an extended failure of that asset could very well have profound adverse consequences for the stability, and even the viability, of the U.S. economy or national security.[24]

[24] Note that the BPS Transmission grid in the area hardest hit by Hurricane Katrina was restored within six days following the storm, but that did not help get municipal water department pumps back up and running because the Distribution systems were still off-line. The public in many hurricane-affected areas did not have running water for a considerable period of time. A hacker incursion resulting in disability of a Distribution control system(s), and/or key assets thereby managed, can be a BPS-independent event that still results in, by example, the pumps of an urban water system being disabled with the same adverse end result for the public. In this specific example, reliable delivery of power to the water infrastructure is also a health and safety issue, not just an inconvenience for the public.

If the overarching objective of the national electric power system is to generate, transmit, and reliably deliver electricity all the way out to the eventual end user – the public – then there are more links in this mission-chain than just the BPS, and the CIP Standards fall short of the mark. To enhance our homeland security, I believe this fundamental issue must be addressed in legislation. I believe this is the most significant difference between the approach set forth in H.R. 2195 and related legislation, H.R. 2165.

V. Conclusion

Thank you for allowing me the opportunity to submit comments to you today on such an important matter facing our nation. I look forward to working with this Committee on these and other homeland security issues in the future.

Mr. MARKEY. And all members can introduce their statements for that purpose.

[The prepared statements of Messrs. Green and Burgess follow:]

Congressman Gene Green
Energy and Environment Subcommittee Hearing
"Protecting the Electric Grid: H.R. 2165, the Bulk Power System Protection Act of 2009, and H.R. 2195"
October 27, 2009

Mr. Chairman, thank you for holding today's hearing on "Protecting the Electric Grid."

As technologies evolve and our electric grid becomes increasingly interconnected via computer systems and Internet-based communications, so too must strategies evolve to protect our infrastructure against any malicious security attack from terrorists, criminal groups, hackers or other potential adversaries.

These threats are not simply theoretical. The Wall Street Journal reported in April that cyber-spies from Russia and China may have infiltrated the U.S. electrical grid and left behind software tools that could be used to damage or destroy critical infrastructure components.

In addition, reports by the Government Accountability Office, the Defense of Defense, and the Department of Homeland Security also identified grid security vulnerabilities that raise questions as to whether our current security regime is sufficient to meet today's growing threats, including those from an electromagnetic pulse (EMP).

The Energy Policy Act of 2005 provides for mandatory reliability standards addressing cyber-security threats for the bulk power system.

Under this authority, the North American Electric Reliability Corporation (NERC) -- which represents electric utilities and stakeholders -- developed nine mandatory Reliability Standards for Critical Infrastructure Protection which FERC has approved with some modifications.

While a strong first step, many industry and governmental experts believe these reliability standards must be strengthened in order to better identify critical assets and respond to imminent cyber security threats.

Many fundamental questions must first be fleshed out, including: whether any new FERC authorities should be harmonized with the Reliability Standards process; whether new authorities should be limited to Bulk Power System owners and operators; whether protection should extend to physical security threats; and whether all electric generators will be able to recover security investment costs.

I look forward to learning more about how we can address the grid's security threats from our distinguished panel of witnesses today, as well to learn more about H.R. 2195 and H.R. 2165, introduced by my good friend Rep. John Barrow.

Thank you Mr. Chairman. I yield back.

Congressman Michael C. Burgess, M.D.
Opening Statement
Subcommittee on Energy & Environment
Hearing on "Protecting the Electric Grid: H.R. 2165, The Bulk Power System Protection Act of 2009, and H.R. 2195"

Thank you, Mr. Chairman.

I will keep my remarks brief today because of the importance of the matter before us. The security of our nation's electricity grid – literally the lifeblood of our economy and society – is of critical importance. Members of this Committee have been briefed, both in classified and unclassified settings, of just how vulnerable certain sectors of our electric grid really are. 8 years after the tragic events of September 11, 2009, this is obviously unacceptable.

Legislation to address the vulnerabilities that we will be discussing today is long overdue. Indeed, rather than spending time writing duplicative and disastrous environmental regulations under the guise of national security legislation, as this Committee has been

doing for the past few weeks, this is the legislation we should have been focusing on, and I'm encouraged that we are taking the first steps toward a full and open markup, including amendments.

While I am a firm believer that the electric grid is most effectively maintained at the state level, where local Public Utility Commissions will always be more responsive to citizens' concerns than the Federal Government, I do agree with my colleagues that within the realm of national security, a greater role for the Federal Government is necessary. I hope that much of the discussion today will focus on exactly where the balance between state and federal authority should properly be.

I further share the concerns of many of my colleagues, as well as members of the industry, as to how to properly address the cost of any increased security measures. At a time when our economy is so fragile, this Committee must consider how costs will affect both the utility companies and the consumers whom they serve, whether

or not the utilities are in a state which regulates the rates consumers pay for electricity. I hope that we may have a fruitful discussion on how best to fund these security measures.

As this country moves forward in updating the electric grid to a more advanced model, increased threats are possible. Our vigilance in protecting the power lines which feed our homes and businesses must be as strong as our focus on the nation's border and port security. I look forward to discussing with the panel just how to go about achieving this goal in the most effective way possible.

With that Mr. Chairman, I yield back.

Mr. MARKEY. I would also like to add that Chairwoman Yvette Clarke of the relevant committee on the Homeland Security Committee and Jim Langevin, who was the Chair last year, would also like to have permission to have space reserved in the record for their statements, as well. And I want to congratulate them on their excellent work on this issue.

[The prepared statement of Mr. Langevin follows:]

Statement of James R. Langevin
Chairman, Subcommittee on Strategic Forces
U.S. House of Representatives House Armed Services Committee

Hearing before the House Committee on Energy and Commerce
Subcommittee on Energy and Environment
October 27, 2009

I would like to thank Chairman Markey for allowing me to testify on the critically important issue of securing our electric grid from cyber vulnerabilities. The Chairman's attention, and the work of his staff, is greatly appreciated and will help highlight the urgency of this issue. I would also like to thank Chairman Thompson of the Homeland Security Committee for his leadership on cybersecurity issues and specifically for continuing to advocate for legislation that I worked with him last year to introduce, H.R. 2195, a bill that will amend the Federal Power Act and provide additional authorities that are necessary to adequately protect the critical electric infrastructure against cyber attack.

Eleven years ago, the President's Commission on Critical Infrastructure Protection released a report on the risks associated with interconnected computer systems on the bulk power system. The Commission stated that "the widespread and increasing use of supervisory control and data acquisition systems for control of energy systems provides increasing ability to cause serious damage and disruption by cyber means."

Since the release of that study, numerous unintentional cyber incidents – the Davis-Besse power plant incident in 2003; the Northeast blackout in 2003; and the Browns Ferry nuclear power shutdown in 2006, to name a few – have confirmed that assertion. Unfortunately, cyber incidents on control systems aren't limited to accidents.

Press reports have emerged about unclassified incidents, such as the interruption of air traffic communications in Massachusetts; the infamous Australian sewage spill perpetrated by an employee of a sewage treatment plant; and the April *Wall Street Journal* report that hackers had penetrated the U.S. electrical grid.

We know that there are a number of actors who seek to do harm to our networks -- from foreign nation states, to domestic criminals and hackers, to disgruntled employees. And as vulnerability and capability grow, so does the ease of attacking our critical infrastructure.

This threat is not new. Last year, on September 11th, 2008, I testified before this Subcommittee about the threats to our bulk power system from cyber attack. In the 110th Congress, as Chairman of the Homeland Security Subcommittee on Emerging Threats, Cybersecurity, Science and Technology, I conducted a detailed and thorough examination of cyber threats to our critical infrastructure, and I want to reiterate what I made clear last year. I believe America is still vulnerable to a cyber attack against the electric grid that would cause severe damage to not only our critical infrastructure, but also our economy and the welfare of our citizens.

Federal agencies have taken steps to reduce these vulnerabilities, but I am afraid that many in industry – and some in government -- still fail to appreciate the urgency of this threat. Since I began working on this issue, I have been disappointed by the overall lack of serious response and commitment from the private sector. I held a hearing in

2007 examining the threats from an "Aurora"-like attack on our national power grid. At that time industry representatives lied to the Committee about having the situation fully under control. We caught them and they retracted their statements, but this attitude shows how difficult it can be to require and ensure security when it comes to critical infrastructure.

The vast majority of our critical assets are in private hands. In many sectors, private entities are largely self-regulated and are responsible for developing and implementing their own standards according to their own priorities. Because fixing vulnerabilities can be costly, security can find itself in conflict with other priorities like profit, competition and accountability to shareholders. Sadly, the American people are the ones placed at risk when the owners of our critical infrastructure fail to prepare for worst-case scenarios.

I was pleased by the early attention paid to the issue of cybersecurity by the new Obama Administration. Last winter, I worked with members of the transition team to highlight some cyber priorities from a congressional perspective, and it was clear even then that the incoming Administration understood the significance of the threat and planned to focus on the issue. Very soon after taking office, President Obama moved forward with the 60-day cyber review, becoming the first major world leader to take such action.

Unfortunately, months later, I worry that we are losing momentum. President Obama still lacks a cybersecurity coordinator – a position which was a key recommendation of both the Administration's cyber review and of the CSIS Commission on Cybersecurity for the 44th Presidency, which I co-chaired last year. Without a cyber coordinator at the highest level of the Administration, directing the efforts of the entire government, we simply can't address this threat effectively. I know there are urgent competing priorities, like our economy and health care, but our national security leaders must not lose sight of this threat.

Meanwhile, this Committee is considering two bills with a similar goal to protect our nation's power grid, and I applaud the attention being focused on this issue. However, I believe that Chairman Thompson's bill, H.R. 2195, is broader in scope and is the better approach to addressing major threats to our electric grid as a whole. It covers all "critical electric infrastructure," against all known cyber vulnerabilities as well as physical attacks. The bill also gives greater authority to the Department of Homeland Security to perform ongoing threat assessments and make recommendations to FERC, enabling faster response by both government and industry in case of an imminent threat. H.R. 2165, in contrast, covers only the bulk power system, thus excluding critical distribution systems that would leave major cities, like New York and Washington, D.C., unprotected by the broader provisions included in H.R. 2195.

The price of inaction on this issue will make our nation increasingly vulnerable to cyber attacks, from both outside and within. We know the threat exists and we have an

opportunity to address it before any further damage is caused. It is the responsibility of this Congress and this Administration to take the appropriate steps that will protect this nation.

I want to once again thank Chairman Markey for his attention to this important issue and for allowing me to offer my testimony to the Committee. I look forward to working with the Energy and Commerce Committee and to supporting your efforts to continue to raise awareness about securing our critical infrastructure and protecting our citizens from cyber attack. Thank you.

Mr. MARKEY. I note that the gentleman from Pennsylvania, Mr. Pitts, has arrived; Mr. Scalise has arrived.

Would you like to be recognized, Mr. Scalise?

Mr. SCALISE. No, thank you.

Mr. MARKEY. Then we will turn——

Mr. PITTS. I will submit it for the record, Mr. Chairman.

Mr. MARKEY. Then the gentleman from Pennsylvania's statement will be included in the record at the appropriate point.

[The prepared statement of Mr. Pitts was unavailable at the time of printing.]

Mr. MARKEY. So we will turn to our first witness, Mr. Joseph McClelland, director of the Office of Electric Reliability at the Federal Energy Regulatory Commission. Mr. McClelland has led FERC's efforts to approve and enforce mandatory reliability standards for the electric grid.

We thank you for joining us today. Please begin.

STATEMENTS OF JOSEPH MCCLELLAND, DIRECTOR, OFFICE OF ELECTRIC RELIABILITY, FEDERAL ENERGY REGULATORY COMMISSION; THE HON. PATRICIA HOFFMAN, PRINCIPAL DEPUTY ASSISTANT SECRETARY, OFFICE OF ELECTRICITY, U.S. DEPARTMENT OF ENERGY; THE HON. GARRY A. BROWN, CHAIRMAN, NEW YORK PUBLIC SERVICE COMMISSION; DAVID N. COOK, VICE PRESIDENT AND GENERAL COUNSEL, NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION; JOHN DISTASIO, GENERAL MANAGER AND CEO, SACRAMENTO MUNICIPAL UTILITY DISTRICT

STATEMENT OF JOSEPH MCCLELLAND

Mr. MCCLELLAND. Mr. Chairman and members of the subcommittee, thank you for the privilege to appear before you today to discuss the security of the power grid.

My name is Joe McClelland, and I am the director of Office of Reliability for the Federal Energy Regulatory Commission. I am here today as a commission staff witness, and my remarks do not necessarily represent the views of the Commission or any individual commissioner.

In the "Energy Policy Act of 2005," or EPACT of 2005, Congress entrusted the Commission with a major new responsibility: to oversee mandatory, enforceable reliability and cybersecurity standards for the Nation's bulk power system. This authority is new Section 215 of the "Federal Power Act."

Under the new authority, FERC cannot author or modify cybersecurity standards but must select an industry self-regulatory organization, termed the Electric Reliability Organization, or ERO, to perform this task. The ERO develops and proposes cybersecurity standards or modifications for the Commission's review, which it can then either approve or remand. If the Commission approves a proposed cybersecurity standard, it applies to the users, owners, and operators of the bulk power system and becomes mandatory in the United States. If the Commission remands a proposed standard, it is sent back to the ERO for further consideration and work.

The Commission selected the North American Electric Reliability Corporation, or NERC, as the ERO. It is important to note that

FERC's jurisdiction and reliability authority is limited to the, quote, "bulk power system," end quote, as defined in the "Federal Power Act," which excludes Alaska and Hawaii, transmission facilities, and certain large cities such as New York City, and distribution systems.

Pursuant to this duty, in January of 2008 FERC approved eight cybersecurity standards, known as the "Critical Infrastructure Protection Standards," or CIP standards, proposed by NERC while concurrently directing modifications to all of them. Although the existing CIP standards are approved, full implementation of these standards by all entities will not be mandatory until 2010.

The first of several batches of modifications responding to the Commission's directives was approved in September of 2009, although the Commission directed further modifications to the revised standards. It is not yet clear how long it will take for the CIP standards to be modified to eliminate some of the significant gaps in protection within them.

On a related note, as smart grid technology is added to the bulk power system, greater cybersecurity protections will be required, given that this technology provides more access points to attackers and can increase the grid's cyber vulnerabilities. The CIP standards will apply to some but not all smart grid applications.

Physical attacks against the power grid can cause equal or greater destruction than cyber attacks. One example of a physical threat is an electromagnetic pulse, or EMP, event. In 2001, Congress established a commission to assess the threat from EMP. And, in 2004 and again in 2008, the EMP Commission issued its reports.

Among the findings of the reports were that a single EMP attack could seriously degrade or shut down a large part of the electric power grid. Depending upon the attacks, significant parts of the electric infrastructure could be, quote, "out of service for periods measured in months to a year or more," end quote.

In addition to man-made attacks, EMP events are also naturally generated, caused by solar flares and storms disrupting the Earth's magnetic field. Such events can be powerful and can also cause significant and prolonged disruptions to the power grid.

Regardless of whether an EMP event is manmade or occurs naturally, it can cause equal or even greater destruction than a cyber attack, and the Federal Government should have no less ability to protect against it.

In September of this year, FERC initiated a research project with the Oak Ridge National Laboratory to study the events of an EMP event on the United States and to identify mitigation measures to protect against it. DOE and DHS have joined in this study, and we expect to complete it within 6 months.

The standards development system utilized under the "Federal Power Act" develops mandatory reliability standards using an open and inclusive process based on consensus. Although it can be an effective mechanism with dealing with the routine requirements of the power grid, it is too slow, too independent, and too open to address threats to the power grid that endanger national security. FERC's current legal authority is insufficient to assure direct, timely, and mandatory action to protect the grid, particularly where certain information should not be publicly disclosed.

Any new legislation should address several key concerns. First, FERC should be permitted to take direct action before a cyber or physical national security incident has occurred. Second, FERC should be allowed to maintain the appropriate confidentiality of security-sensitive information. Third, the limitations on the term, quote, "bulk power system," end quote, should be considered, as FERC cannot act to protect attacks involving Alaska and Hawaii, as well as some transmission and all local distribution facilities in large-population areas. Finally, if Congress finds it appropriate, Congress should provide a mechanism allowing entities to recover costs that the utilities incur to mitigate vulnerabilities and threats.

Thank you for attention today, and I look forward to any questions that you may have.

[The prepared statement of Mr. McClelland follows:]

Testimony of Joseph McClelland
Director, Office of Electric Reliability
Federal Energy Regulatory Commission
Before the Committee on Energy and Commerce
Subcommittee on Energy and Environment
United States House of Representatives
October 27, 2009

Mr. Chairman and Members of the Subcommittee:

Thank you for this opportunity to appear before you to discuss the security of the electric grid. My name is Joseph McClelland. I am the Director of the Office of Electric Reliability (OER) of the Federal Energy Regulatory Commission (FERC or Commission). The Commission's role with respect to reliability is to help protect and improve the reliability of the Nation's bulk power system through effective regulatory oversight as established in the Energy Policy Act of 2005. I am here today as a Commission staff witness and my remarks do not necessarily represent the views of the Commission or any individual Commissioner.

My testimony summarizes the Commission's oversight of the reliability of the electric grid under section 215 of the Federal Power Act, and some of the limitations in Federal authority to protect the grid against physical and cyber security threats. The Commission currently does not have sufficient authority to require effective protection of the grid against cyber or physical attacks. If adequate protection is to be provided, legislation is needed and my testimony discusses the key elements that should be included in any new legislation in this area.

Background

In the Energy Policy Act of 2005 (EPAct 2005), Congress entrusted the Commission with a major new responsibility to oversee mandatory, enforceable reliability standards for the Nation's bulk power system (excluding Alaska and Hawaii). This authority is in section 215 of the Federal Power Act. Section 215 requires the Commission to select an Electric Reliability Organization (ERO) that is responsible for proposing, for Commission review and approval, reliability standards or modifications to existing reliability standards to help protect and improve the reliability of the Nation's bulk power system. The Commission has certified the North American Electric Reliability Corporation (NERC) as the ERO. The reliability standards apply to the users, owners and operators of the bulk power system and become mandatory in the United States only after Commission

approval. The ERO also is authorized to impose, after notice and opportunity for a hearing, penalties for violations of the reliability standards, subject to Commission review and approval. The ERO may delegate certain responsibilities to "Regional Entities," subject to Commission approval.

The Commission may approve proposed reliability standards or modifications to previously approved standards if it finds them "just, reasonable, not unduly discriminatory or preferential, and in the public interest." The Commission itself does not have authority to modify proposed standards. Rather, if the Commission disapproves a proposed standard or modification, section 215 requires the Commission to remand it to the ERO for further consideration. The Commission, upon its own motion or upon complaint, may direct the ERO to submit a proposed standard or modification on a specific matter but it does not have the authority to modify or author a standard and must depend upon the ERO to do so.

Limitations of Section 215 And The Term "Bulk Power System"

Currently, the Commission's jurisdiction and reliability authority is limited to the "bulk power system," as defined in the FPA, and therefore excludes Alaska and Hawaii, including any federal installations located therein. The current interpretation of "bulk power system" also excludes some transmission and all local distribution facilities, including virtually all of the grid facilities in certain large cities such as New York, thus precluding Commission action to mitigate cyber or other national security threats to reliability that involve such facilities and major population areas.

Critical Infrastructure Protection Reliability Standards

An important part of the Commission's current responsibility to oversee the development of reliability standards for the bulk power system involves cyber security. In August 2006, NERC submitted eight proposed cyber security standards, known as the Critical Infrastructure Protection (CIP) standards, to the Commission for approval under section 215. Critical infrastructure, as defined by NERC for purposes of the CIP standards, includes facilities, systems, and equipment which, if destroyed, degraded, or otherwise rendered unavailable, would affect the reliability or operability of the "Bulk Electric System." NERC proposed an implementation plan under which certain requirements would be "auditably compliant" beginning by mid-2009, and full compliance would be mandatory in 2010. Pursuant to NERC's implementation plan for the CIP standards, the term "auditably compliant" means "the entity meets the full intent of the requirement and can demonstrate compliance to an auditor, including 12-calendar-months of auditable 'data,' 'documents,' 'documentation,' 'logs,' and 'records.'"

On January 18, 2008, the Commission issued Order No. 706, the Final Rule approving the CIP reliability standards while concurrently directing NERC to develop significant modifications addressing specific concerns. The Commission set a deadline of July 1, 2009 for NERC to resolve certain issues in the CIP reliability standards, including deletion of the "reasonable business judgment" and "acceptance of risk" language in each of the standards. NERC concluded that this deadline would create a very compressed schedule for its stakeholder process. Therefore, it divided all of the changes directed by the Commission into phases, based on their complexity. NERC opted to resolve the simplest changes in the first phase, while putting off more complex changes for later versions.

NERC filed the first phase of the modifications to the CIP Reliability Standards (Version 2) on May 22, 2009. In this phase, NERC removed from the standards the terms "reasonable business judgment" and "acceptance of risk," added a requirement for a "single senior manager" responsible for CIP compliance, and made certain other administrative and clarifying changes. In a September 30, 2009 order, the Commission approved the Version 2 standards and directed NERC to develop additional modifications to certain of them. Pursuant to NERC's request, the Version 2 standards will become effective on April 1, 2010, in order to allow registered entities a period of time to comply. The remaining phases of the CIP standard revisions to respond to the Commission's directives are still under development by NERC. It is important to note that the majority of the changes to the standards directed by the Commission have yet to be addressed by NERC. Until they are addressed, there are significant gaps in protection such as self-determination of the assets covered by the CIP standards, a needed framework for oversight and approval of technical feasibility exceptions, and a needed requirement for a defense in depth posture. To address these outstanding items, in the September 30, 2009 order, the Commission ordered NERC to provide a timetable that reflects its plan to address the remaining modifications directed by the Commission in the Final Rule. The Commission expects NERC to file its implementation plan by the beginning of next year.

Identification of Critical Assets

As currently written, the CIP reliability standards allow utilities significant discretion to determine which of their facilities are "critical assets and the associated critical cyber assets," and therefore are subject to the protection requirements of the standards. In the Final Rule, the Commission directed NERC to revise the standards to require independent oversight of a utility's decisions by industry entities with a "wide-area view," such as reliability coordinators or the Regional Entities, subject to the review of the Commission. This revision to the standards, like all revisions, is subject to approval by the affected stakeholders in the standards development process and has not yet been developed. We expect

this revision to be part of the remaining phases of CIP reliability standard revisions, as discussed above.

When the Commission approved the CIP reliability standards in January 2008, it also required entities under those standards to self-certify their compliance progress every six months. In December 2008, NERC conducted a self-certification study, asking each entity to report limited information on its critical assets and the associated critical cyber assets identified in compliance with reliability standard CIP-002-1. As the Commission stated in the Final Rule, the identification of critical assets is the cornerstone of the CIP standards. If that identification is not done well, the CIP standards will be ineffective at protecting the bulk power system. The results of NERC's self-certification request showed that 31% of responsible entities responding to the survey, and only 29% of responding generation owners and operators, identified at least one critical asset, while about 63% of transmission owners identified at least one critical asset. NERC expressed its concern with these results in a letter to industry stakeholders dated April 7, 2009.

NERC has sent a second self-certification survey to responsible entities to determine progress towards identification of critical cyber assets. This survey includes additional questions designed to obtain a better understanding of the results from industry's critical asset identification process. Those results will help gauge how widely the CIP reliability standards have been applied. Commission staff understands that NERC is currently reviewing the responses to the survey and expects the results to be presented to the Commission shortly. In addition, the Regional Entities have been performing audits which have included registered entities' determination of their critical cyber asset lists. FERC staff has been observing selected audits to examine the Regional Entities' methods of conducting these audits.

Recently, NERC's Critical Infrastructure Protection Committee released a guidance document to assist registered entities in identifying their critical assets. That document, which took effect on September 17, 2009, provides "guidelines" that define which assets should be evaluated, provides risk-based evaluation guidance for determining critical assets, and describes reasonable bases that could be used to support that determination. In addition, in an effort to consider a new approach to determining critical cyber assets under the CIP-002 standard, the NERC standards development team has released a concept paper that explores a new methodology, one which first identifies all cyber systems that support the reliable operation of the bulk power system and then categorizes each system based on its impact. Cyber protection requirements would then be commensurate with the level of potential impact.

At this point, however, it is clear that all critical assets and associated critical cyber assets have not been identified and therefore made subject to the protection requirements of the CIP standards. This represents a significant gap in cyber security protection.

The NERC Process

As an initial matter, it is important to recognize how mandatory reliability standards are established. Under section 215, reliability standards must be developed by the ERO through an open, inclusive, and public process. The Commission can direct NERC to develop a reliability standard to address a particular reliability matter, including cyber security threats or vulnerabilities. However, the NERC process typically requires years to develop standards for the Commission's review. In fact, the CIP standards approved by the Commission in January 2008 took approximately three years to develop.

NERC's procedures for developing standards allow extensive opportunity for stakeholder comment, are open, and are generally based on the procedures of the American National Standards Institute. The NERC process is intended to develop consensus on both the need for, and the substance of, the proposed standard. Although inclusive, the process is relatively slow, open and unpredictable in its responsiveness to the Commission's directives.

Key steps in the NERC process include: nomination of a proposed standard using a Standard Authorization Request (SAR); public posting of the SAR for comment; review of the comments by industry volunteers; drafting or redrafting of the standard by a team of industry volunteers; public posting of the draft standard; field testing of the draft standard, if appropriate; formal balloting of the draft standard, with approval requiring a quorum of votes by 75 percent of the ballot pool and affirmative votes by two-thirds of the weighted industry sector votes; re-balloting, if negative votes are supported by specific comments; approval by NERC's board of trustees; and an appeals mechanism to resolve any complaints about the standards process. This process requires public disclosure regarding the reason for the proposed standard, the manner in which the standard will address the issues, and any subsequent comments and resulting modifications in the standards as the affected stakeholders review the material and provide comments. NERC-approved standards are then submitted to the Commission for its review.

Generally, the procedures used by NERC are appropriate for developing and approving reliability standards. The process allows extensive opportunities for industry and public comment. The public nature of the reliability standards development process can be a strength of the process. However, it can be an impediment when measures or actions need to be taken to address threats to national security quickly, effectively and in a manner that protects against the

disclosure of security-sensitive information. The current procedures used under section 215 for the development and approval of reliability standards do not provide an effective and timely means of addressing urgent cyber or other national security risks to the bulk power system, particularly in emergency situations. Certain circumstances, such as those involving national security, may require immediate action, while the reliability standard procedures take too long to implement efficient and timely corrective steps.

FERC rules governing review and establishment of reliability standards allow the agency to direct the ERO to develop and propose reliability standards under an expedited schedule. For example, FERC could order the ERO to submit a reliability standard to address a reliability vulnerability within 60 days. Also, NERC's rules of procedure include a provision for approval of "urgent action" standards that can be completed within 60 days and which may be further expedited by a written finding by the NERC board of trustees that an extraordinary and immediate threat exists to bulk power system reliability or national security. However, it is not clear NERC could meet this schedule in practice. Moreover, faced with a national security threat to reliability, there may be a need to act decisively in hours or days, rather than weeks, months or years. That would not be feasible even under the urgent action process. In the meantime, the bulk power system would be left vulnerable to a known national security threat. Moreover, existing procedures, including the urgent action procedure, would widely publicize both the vulnerability and the proposed solutions, thus increasing the risk of hostile actions before the appropriate solutions are implemented.

In addition, a reliability standard submitted to the Commission by NERC may not be sufficient to address the identified vulnerability or threat. Since FERC may not directly modify a proposed reliability standard under section 215 and must either approve or remand it, FERC would have the choice of approving an inadequate standard and directing changes, which reinitiates a process that can take years, or rejecting the standard altogether. Under either approach, the bulk power system would remain vulnerable for a prolonged period.

Finally, the open and inclusive process required for standards development is not consistent with the need to protect security-sensitive information. For instance, a Standard Authorization Request would normally detail the need for the standard as well as the proposed mitigation to address the issue, and the NERC-approved version of the standard would be filed with the Commission for review. This public information could help potential adversaries in planning attacks.

NERC's "Aurora" Advisory

Currently, the alternative to a mandatory reliability standard is for NERC to issue an advisory encouraging utilities and others to take voluntary action to guard

against cyber or other vulnerabilities. That approach allows for quicker action, but compliance with an advisory is voluntary, and will likely produce inconsistent and potentially ineffective responses. By its nature, an alert can be general in nature and lack specificity. For example, the issuance of an advisory in 2007 by NERC, regarding an identified cyber security vulnerability referred to as "Aurora," resulted in differing strategies and compliance actions to mitigate the identified vulnerabilities and the assets to which they apply. Reliance on voluntary measures to protect national security is fundamentally inconsistent with the conclusion Congress reached during enactment of EPAct 2005, that voluntary standards are not sufficient to protect the reliability of the bulk power system.

Smart Grid

The need for vigilance will increase as new technologies are added to the bulk power system. For example, smart grid technology promises significant benefits in the use of electricity. These include the ability to better manage not only energy sources but also energy consumption. However, a smarter grid would permit two-way communication between the electric system and a large number of devices located outside of controlled utility environments, which will introduce many potential access points.

Smart grid applications will automate many decisions on the supply and use of electricity to increase efficiencies and ultimately to allow cost savings. Without adequate physical and cyber protections, however, this level of automation may allow adversaries to gain access to the rest of the company's data and control systems and cause significant harm. Security features must be an integral consideration when developing smart grid technology and must be assured before widespread installation of new equipment. The challenge will be to focus not only on general approaches but, importantly, on the details of specific technologies and the risks they may present.

Regarding data, there are multiple ways in which smart grid technologies may introduce new cyber vulnerabilities into the system. For example an attacker could gain access to a remote or intermediate smart grid device and change data values monitored or received from down-stream devices, and pass the incorrect data up-stream to cause operators or automatic programs to take incorrect actions. As was mentioned previously, the potential exists for off-grid equipment to adversely affect the bulk power system through corrupted communications.

In regard to control systems, an attacker that gains access to the communication channels could order metering devices to disconnect customers, order previously shed load to come back on line prematurely, or order dispersed generation sources to turn off during periods when load is approaching generation capacity, causing instability and outages on the bulk power system. One of the

potential capabilities of the smart grid is the ability to remotely disconnect service using advanced metering infrastructure (AMI). If insufficient security measures are implemented in a company's AMI application, an adversary may be able to access the AMI system and could conceivably disconnect every customer with an AMI device. If such an attack is widespread enough, the resultant disconnection of load on the distribution system could result in impacts to the bulk power system. If an adversary follows this disconnection event with a subsequent and targeted cyber attack against remote meters, the restoration of service could be greatly delayed.

The CIP standards will apply to some, but not all, smart grid applications. The standards require users, owners and operators of the bulk power system to protect cyber assets, including hardware, software and data, which would affect the reliability or operability of the bulk power system. These assets are identified using a risk-based assessment methodology that identifies electric assets that are critical to the reliable operation of the bulk power system. If a smart grid device were to control a critical part of the bulk power system, it should be considered a critical cyber asset subject to the protection requirements of the CIP standards. However, this designation is currently up to the affected entity as part of its self-determination of critical cyber assets, as discussed previously.

Many of the smart grid applications will be deployed at the distribution and end-user level so they may incorrectly be viewed as not affecting the bulk power system. For example, some applications may be targeted at improving market efficiency in ways that may not have a reliability impact on the bulk power system, such that the protection requirements of the CIP standards, as they are currently written, may not apply. However, as discussed above, these applications either individually or in the aggregate could affect the bulk power system.

The Commission and its staff currently are coordinating with a number of governmental and private sector organizations on cyber security issues surrounding smart grid technology, including the DOE Smart Grid Task Force, the NIST Domain Expert Working Groups, the Gridwise Architecture Council, and the FERC-NARUC Smart Grid Collaborative. The Commission has issued a policy statement that would strongly encourage interoperability of smart grid technologies, recognizing that cyber security is essential to the operation of the smart grid. The Commission also encouraged NERC to work with NIST in the development of the standards.

While the Commission is doing what it can under its jurisdiction, the Energy Independence and Security Act of 2007 does not make any standards mandatory and does not give the Commission authority to make or enforce any

such standards. Under current law, the Commission's authority, if any, to make smart grid standards mandatory must derive from the FPA.

Physical Security And Other Threats To Reliability

The existing reliability standards do not extend to physical threats to the grid, but physical threats can cause equal or greater destruction than cyber attacks and the Federal government should have no less ability to act to protect against such potential damage. One example of a physical threat is an electromagnetic pulse (EMP) event. In 2001, Congress established a commission to assess the threat from EMP, with particular attention to be paid to the nature and magnitude of high-altitude EMP threats to the United States; vulnerabilities of U.S. military and civilian infrastructure to such attack; capabilities to recover from an attack; and the feasibility and cost of protecting military and civilian infrastructure, including energy infrastructure. In 2004, the EMP commission issued a report describing the nature of EMP attacks, vulnerabilities to EMP attacks, and strategies to respond to an attack.[1] A second report was produced in 2008 that further investigated vulnerabilities of the Nation's infrastructure to EMP.[2] Both electrical equipment and control systems can be damaged by EMP.

An EMP may also be a naturally-occurring event caused by solar flares and storms disrupting the Earth's magnetic field. In 1859, a major solar storm occurred, causing auroral displays and significant shifts of the Earth's magnetic fields. As a result, telegraphs were rendered useless and several telegraph stations burned down. The impacts of that storm were muted because semiconductor technology did not exist at the time. Were the storm to happen today, according to an article in *Scientific American*, it could "severely damage satellites, disable radio communications, and cause continent-wide electrical black-outs that would require weeks or longer to recover from."[3] Although storms of this magnitude occur rarely, storms and flares of lesser intensity occur more frequently. Storms of about half the intensity of the 1859 storm occur every 50 years or so according to the authors of the *Scientific American* article, and the last such storm occurred in

---

[1] Graham, Dr. William R. et al., *Report of the Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack* (2004).

[2] Foster, Dr. John S., Jr. et al., *Report of the Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack* (2008).

[3] Odenwald, Sten F. and Green, James L., *Bracing the Satellite Infrastructure for a Solar Superstorm*, Scientific American Magazine (Jul. 28, 2008).

November 1960, leading to world-wide geomagnetic disturbances and radio outages.

The power grid is particularly vulnerable to solar storms, as transformers are electrically grounded to the Earth and susceptible to damage from geomagnetically induced currents. The damage or destruction of numerous transformers across the country would result in reduced grid functionality and even prolonged power outages.

FERC staff has no data on how well the bulk power system is protected against an EMP event, and the existing reliability standards do not address EMP vulnerabilities. Further, the Commission currently does not have any specific authority to order owners and operators of the transmission grid, generation facilities and other electric facilities to protect their facilities from EMP-related events, other than the general authority to order NERC to develop a reliability standard addressing EMP. Protecting the electric generation, transmission and distribution systems from severe damage due to an EMP-related event would involve vulnerability assessments at every level of electric infrastructure. In addition, as the EMP commission reports point out, the reliable operation of the electric grid requires other infrastructure systems, such as communications, natural gas pipelines and transportation, which would also be affected by such an attack or event.

To further explore the vulnerability of the electric grid due to EMP-related events as well as potential mitigation of those events, FERC staff, along with the Department of Energy and the Department of Homeland Security, has recently initiated a joint study with Oak Ridge National Laboratory (Oak Ridge) and subcontractor Metatech. The Oak Ridge contract will expand on the materials developed in other initiatives, including the EMP commission reports, with emphasis on which sections of the power grid are most vulnerable, what equipment would be affected, and what the resulting damage would do. The contractor will describe protection concepts for each threat, as well as evaluating additional methods for remediation. Finally, the contractor will provide specific mitigation recommendations which can be used to develop and test hardware prototypes and operational procedures to establish the effectiveness and cost of mitigation to achieve protection for the Nation's power grid against these intense electromagnetic threats. Oak Ridge began work on the contract on October 1, 2009 and is expected to complete it by March, 2010.

The Need for Legislation

In my view, section 215 of the Federal Power Act provides an adequate statutory foundation for the ERO to develop most reliability standards for the bulk power system. However, the nature of a national security threat by entities intent

on attacking the U.S. through vulnerabilities in its electric grid stands in stark contrast to other major reliability vulnerabilities that have caused regional blackouts and reliability failures in the past, such as vegetation management and protective relay maintenance practices. Widespread disruption of electric service can quickly undermine the U.S. government, its military, and the economy, as well as endanger the health and safety of millions of citizens. Given the national security dimension to this threat, there may be a need to act quickly to protect the grid, to act in a manner where action is mandatory rather than voluntary, and to protect certain information from public disclosure.

The Commission's current legal authority is inadequate for such action. This is true of both cyber and physical threats to the bulk power system that pose national security concerns. Further, although section 202(c) of the FPA provides the Department of Energy certain emergency authority, in my view that authority is not adequate to cover the types of actions that might need to be ordered to protect the electric grid. Simply put, the federal government at this time does not have sufficient ability to timely protect the electric grid against cyber or physical attacks.

Any new legislation should address several key concerns. First, to prevent a significant risk of disruption to the grid, legislation should allow the Commission to take action before a cyber or physical national security incident has occurred. The Commission has the expertise to determine what actions are necessary to protect the electric grid and it is vital that it be authorized to act before an attack occurs. The Commission is not the appropriate agency to determine whether a national security threat exists. However, once DOE or another national security agency does make that determination, the Commission, in consultation with other agencies and industry as appropriate, must be able to timely order the actions necessary to protect the grid.

Second, any legislation should allow the Commission to maintain appropriate confidentiality of sensitive information submitted, developed or issued under this authority. Without such confidentiality, the grid may be more vulnerable to attack and the Commission will not be able to adequately protect it.

Third, it is important that Congress be aware that if additional reliability authority is limited to the bulk power system, as that term is currently defined in the FPA, it would exclude protection against attacks involving Alaska and Hawaii, including any federal installations located therein. The current interpretation of the term bulk power system also excludes some transmission and all local distribution facilities, including virtually all of the facilities in certain large cities such as New York, thus precluding possible Commission action to mitigate cyber or other national security threats to reliability that involve such facilities and major population areas.

Fourth, it is important that entities be permitted to recover costs they incur to mitigate vulnerabilities and threats. The Commission currently has authority to allow recovery by entities that meet the FPA definition of "public utility." If Congress believes it appropriate, it should include in legislation a directive that the Commission establish a cost recovery mechanism for the costs associated with compliance with any FERC order issued pursuant to the emergency authority.

Finally, in my view, any legislation on national security threats to reliability should address not only cyber security threats but also intentional physical malicious acts (targeting, for example, critical substations and generating stations) including threats from an electromagnetic pulse. FERC should be granted authority to address both cyber and physical threats and vulnerabilities, primarily because FERC is the one Federal agency with any statutory responsibility to oversee the reliability of the grid. This additional authority would not displace other means of protecting the grid, such as action by federal, state and local law enforcement and the National Guard. If particular circumstances cause both FERC and other governmental authorities to require action by utilities, FERC would coordinate with other authorities as appropriate.

Conclusion

The Commission's current authority is not adequate to address cyber or other national security threats to the reliability of our transmission and power system. These types of threats pose an increasing risk to our Nation's electric grid, which undergirds our government and economy and helps ensure the health and welfare of our citizens. Congress should address this risk now. Thank you again for the opportunity to testify today. I would be happy to answer any questions you may have.

Mr. MARKEY. Great. Thank you, Mr. McClelland, very much.

And I will say to each one of you that you only have 5 minutes for your opening statement. And after I introduce you, you don't have to read that part of your statement again. You can get right to the meat of it, oK, because I will have done it.

Our next witness is Ms. Patricia Hoffman, principal deputy assistant secretary of the Office of Electricity at the U.S. Department of Energy. In this capacity, Ms. Hoffman provides leadership on a national level to modernize the electric grid and enhance the security and reliability of the energy infrastructure.

Thank you for joining us today. Whenever you are ready, please begin.

STATEMENT OF THE HON. PATRICIA HOFFMAN

Ms. HOFFMAN. Thank you, Chairman Markey and members of the subcommittee, for this opportunity to testify before you today on H.R. 2195 and 2165.

The energy sector's threat analysis encompasses natural events, criminal acts, and insider threats, as well as foreign and domestic terrorism. Because of the diversity of assets in the systems in the energy sector, a multitude of methodologies have been used to assess risks, vulnerabilities, and consequences.

Also, improving the resiliency of the Nation's electric power grid for the purpose of national security will come at a cost. As Congress considers legislation, we recognize there are limited resources. Therefore, we must prioritize our activities, continually assessing risk, the impact to the electric sector, and financial impacts.

Incident response and information sharing still remain foremost our concern. While the United States has had a good deal of experience with physical disruptions to the grid, such as the 2003 Northeast blackout and the hurricanes of 2005 and 2008, it does not have experience-based lessons learned from a cyber incident. While coordination and communication has improved between public and private organizations over the past several years, much more is needed to prevent and respond to an attack that could hamper the U.S. electric power grid.

The 2010 Energy and Water Appropriations Conference Report directs the Department of Energy to develop an independent national energy-sector cybersecurity organization to institute research; development and deployment priorities, including policies and protocols to ensure the effective deployment of tested and validated technology and software controls to protect the bulk power system; and the integration of smart technologies to enhance the security of the electric grid.

Congress assigned the National Institute of Standards and Technology, NIST, with the responsibility to coordinate the development of a framework and a roadmap for interoperability standards, including cybersecurity. The Department has been working closely with NIST and other agencies through this Smart Grid Task Force and the private sector. I am pleased to say significant progress has been made. NIST issued Release 1.0 of the "NIST Framework and Roadmap for Smart Grid Interoperability Standards," as well as

Draft NIST Interagency Report 7628, "Smart Grid Cybersecurity Strategy and Requirements."

The Department recognizes the inherent weaknesses associated with driving system effectiveness and risk from a single worst-case scenario. A single worst-case scenario is possible but rarely exists and often exceeds the known and projected adversary capabilities. At the same time, focusing on the worst-case scenario may result in overlooking protection system elements needed to counter more probable, significant, and credible threats. Consequently, the Department is looking at a more balanced methodology to effectively detect and deter threats.

The Department reviewed the various bills and conducted analysis to evaluate the effectiveness. We also have reviewed the existing cybersecurity standards and the relative effectiveness in addressing high-consequence risks in a rapidly changing threat environment.

The Department provides the committee the following technical comments.

The Federal Energy Regulatory Commission could be authorized to issue an emergency security directive to owners and operators of the bulk power system covering a specific period of time if the Secretary of Energy has determined that a power grid emergency exists.

A power grid emergency could be defined as a situation that poses a high risk to the bulk power system that must be addressed within 60 days without public disclosure. Determination of a power grid emergency in general would require the expertise of the Secretary of Energy, in consultation with the Secretary of Homeland Security, the Office of Attorney General, and the Director of National Intelligence.

In making a determination, the Secretary could consider: a known cyber vulnerability exists that may affect the bulk power system; a threat actor is determined to have known or suspected intent, requisite resources, and capabilities to carry out the threat with a high likelihood; if exploited, the vulnerability would result in significant consequences, including damage to assets, infrastructure, loss of life, and psychological damage; the situation presents an imminent risk to the bulk power system.

Any directive should have performance objectives and metrics for mitigating the identified threat vulnerability and/or potential consequence. The directive may alternately be in the form of an alert that notify owners or operators of a potentially serious cyber situation. Specific methods for compliance could be left to the discretion of the provider of the bulk electric power, provided the security performance objectives are met.

Any directives should notify private-sector operators of the bulk power system of the nature of the risk, consistent with the proper handling of classified and restricted information, and direct operators to investigate, take appropriate and corrective action, and file report findings back to FERC within a specified time period; and, if required, direct owners and operators of the bulk power system through NERC to develop mitigations to test and validate such mitigations. The Department of Energy could provide technical support.

With this, I will conclude my testimony. I thank you for the opportunity for being here, and I look forward to any questions you have.

[The prepared statement of Ms. Hoffman follows:]

STATEMENT OF
PATRICIA HOFFMAN
ACTING ASSISTANT SECRETARY
FOR ELECTRICITY DELIVERY AND ENERGY RELIABILITY
U.S. DEPARTMENT OF ENERGY

BEFORE THE
ENERGY AND COMMERCE COMMITTEE
ENERGY AND ENVIRONMENT SUBCOMMITTEE
UNITED STATES HOUSE OF REPRESENTATIVES
October 27, 2009

Thank you Chairman Markey and members of the Subcommittee for this opportunity to testify before you on emergency security directives and electric system reliability.

All of us here today have a common goal—ensuring the resiliency of the Nation's electric power grid. We all understand that vulnerabilities exist within the electric system and that the Department of Energy, in partnership with the rest of the Federal Government and power industry, should work towards implementing the "Roadmap to Secure Control Systems for the Energy Sector." [1]

The energy sector's threat analysis encompasses natural events, criminal acts, and insider threats, as well as foreign and domestic terrorism. Because of the diversity of assets and systems in the energy sector, a multitude of methodologies have been used to assess risks, vulnerabilities, and consequences.

Also to note, improving the resiliency of the Nation's electric power grid for the purpose of national security comes at a cost. New transformers can be electromagnetic pulse (EMP)-hardened for a very small fraction of the cost of the non-hardened item, e.g. one percent to three percent of cost, if hardening is done at the time the unit is designed and manufactured. In contrast, retrofitting existing functional components is potentially an order of magnitude more.[2] As Congress considers legislation, we recognize there are limited resources. Therefore we must prioritize based on risk, impact to the electric system and cost constraints.

---

[1] Department of Energy in collaboration with Department of Homeland Security and the Natural Resources Technology Directorate and the Energy Infrastructure Protection Division of Natural Resources Canada, 2006.

[2] Report of the Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack, 2004.

Vulnerabilities

The exploitation of high-risk vulnerabilities has become one of the greatest concerns for potential disruption. Control systems networks provide great efficiency and are widely used. However, they also present a security risk, if not adequately protected. Many of these networks were initially designed to maximize functionality and cost effectiveness, with little attention paid to security. With connections to the Internet, internal local area and wide area networks, wireless network devices, and modems, some networks are potentially vulnerable to disruption of service, process redirection, or manipulation of operational data that could cause disruptions to the Nation's critical infrastructure.

The United States Government is also considering the effect of High Impact-Low Frequency (HILF) events on our Nation's electric system. The Department is working with the North American Electric Reliability Corporation (NERC) to examine the effects of HILF events on the bulk power system. The effort will focus on HILF events such as influenza pandemic, space weather, terrorist attacks and electromagnetic pulses.

In addition, the Department, the Federal Energy Regulatory Commission (FERC), and the Department of Homeland Security (DHS), are funding an EMP study. The study will focus on electromagnetic threats and how they relate to the reliable operation of the U.S. electric power grid. The study will provide specific recommendations for activities to be accomplished in the future to achieve the protection of the U.S. electric power grid.

Incident response and information sharing still remain foremost concern. While the United States has a good deal of experience with physical disruptions to the grid, such as the 2003 Northeast Blackout and the Hurricanes of 2005 and 2008, it does not have experience-based lessons learned from a cyber incident. While coordination and communications have improved between public and private organizations over the past several years, much more is needed to prevent and respond to an attack that could hamper the U.S. electric power grid.

Enhancing the Security of the Energy Sector

For more than a decade, the Department has worked with the private sector to secure the electric grid. In December 2003, the Homeland Security Presidential Directive 7 (HSPD-7) designated the Department as the sector-specific agency (SSA) for the energy sector and provided authorization to collaborate with all Federal agencies, state and local governments, and the private sector, to conduct

vulnerability assessments of the sector, and to encourage risk management strategies for critical energy infrastructure.

The Department takes this responsibility very seriously, and works closely with the private sector and state/Federal regulators to improve secure sharing of threat information and collaborate with the industry to identify and fund gaps in infrastructure research, development and testing efforts.

Our efforts to enhance the cyber security of the energy infrastructure have produced results in four areas. We have:

1. Identified cyber vulnerabilities in energy control systems and worked with vendors to develop hardened systems that mitigate the risks;
2. Developed more secure communications methods between energy control systems and field devices;
3. Developed tools and methods to help utilities assess their security posture; and
4. Provided extensive cyber security training for energy owners and operators to help them prevent, detect, and mitigate cyber penetration.

In 2003, the Department launched its National SCADA Test Bed (NSTB), a state-of-the-art national resource designed to aid government and industry in securing their control systems against cyber attack through vulnerability assessments, mitigation research, security training, and focused R&D efforts. The Department has expanded the NSTB to include resources and capabilities from five national laboratories.

To date, NSTB researchers have assessed the majority of SCADA/Energy Management Systems (SCADA/EMS) being offered in the energy sector. Twenty NSTB and on-site field assessments of common control systems from vendors including ABB, Areva, GE, OSI, Siemens, Telvent, and others, have led vendors to develop 11 hardened control system designs. Today, over 40 of these "hardened" SCADA/EMS systems have been deployed to better protect the power grid from cyber attacks, vendors have also issued many software patches to better secure legacy systems, which are now being used by 82 system applications in the sector. Findings from NSTB vulnerability assessments have also been generalized by Idaho National Laboratory into its *Common Vulnerabilities Report*, which includes mitigation strategies asset owners across the sector can use to better secure their systems.

The FY 2010 Energy and Water Appropriations Conference Report directs the Department to develop an independent national energy sector cyber security organization to institute research, development and deployment priorities,

including policies and protocols to ensure the effective deployment of tested and validated technology and software controls to protect the bulk power electric grid and integration of smart grid technology to enhance the security of the electricity grid. The Department recognizes the importance of an independent organization that includes industry in advancing cyber security and will make establishing this organization a top priority.

Cyber Security and the Smart Grid

Over the last 6 months, the Department has been highly focused on implementing several initiatives set forth in the Recovery Act, including $4.5B for smart grid activities designed to jumpstart the modernization of the electric power grid, reduce electricity use, reduce greenhouse gas emissions, and spur innovation and economic recovery. A key aspect for the implementation of smart grid technologies is the need to address interoperability and cyber security. It is paramount that smart grid devices and interoperability standards include protections against cyber intrusions and have systems that are designed from the start (not patches added on) that prevent unauthorized persons from gaining entry through the millions of new access points created by the deployment of smart grid technologies.

Under EISA Section 1305, Congress assigned the National Institute of Standards and Technology (NIST) with the responsibility to coordinate the development of a framework and roadmap for interoperability standards including cyber security. The Department has been working closely with NIST and other agencies through the Smart Grid Task Force and the private sector, and I am pleased to say significant progress has been made. NIST issued Release 1.0 of the "NIST Framework and Roadmap for Smart Grid Interoperability Standards" as well as Draft NISTIR 7628, "Smart Grid Cyber Security Strategy and Requirements." Recognizing the importance and urgency of cyber security standards for the Smart Grid, in May 2009 the Department partnered with the UCA International Users Group (UCAIug), Consumers Energy, Florida Power & Light, and Southern California Edison and launched the Advanced Security Acceleration Project - Smart Grid (ASAP-SG) specifically to accelerate the development of cyber security standards for the smart grid. ASAP-SG is developing a set of security profiles, each containing a baseline set of security controls for a given smart grid application. These profiles can be used by utilities and vendors to improve the security of smart grid applications and implementations. ASAP-SG is working closely with the NIST Cyber Security Coordination Task Group (CSCTG) and recently delivered an Advance Metering Infrastructure (AMI) security profile which is incorporated in the Draft NISTIR 7628.

Critical Infrastructure Protection and a Threat Analysis Methodology

In the aftermath of 9/11, we have strived to define and implement domestic threat policies that adequately balance the potential consequences associated with the loss/misuse of an asset; limited fiscal and physical resources; the capabilities of the intelligence community to identify threats in a timely manner; the ability of other agencies to interdict emerging threats; and the ability to effectively and quickly respond to constantly changing threats.

The Department recognized the inherent weaknesses associated with deriving system effectiveness and risk from a single "worst-case" scenario. A single "worst-case" scenario is possible, but rarely exists and often exceeds the known and projected adversary capabilities. At the same time, focusing on the "worst-case" scenario may result in overlooking protection system elements needed to counter more probable significant and credible threats. Consequently, the Department required a more balanced methodology to effectively detect and deter the threats.

Technical Comments on H.R 2195 and H.R. 2165

The Department reviewed the various bills and conducted analyses to evaluate effectiveness. We also reviewed existing cyber security standards and their relative effectiveness in addressing high consequence risks in a rapidly changing threat environment. The Department would like to provide the following technical comments:

The Federal Energy Regulatory Commission could be authorized to issue an Emergency Security Directive to owners and operators of the bulk power system, covering a specific period of time, if the Secretary of Energy has determined that a power grid emergency exists.

A "power grid emergency" is defined as a situation that poses a high risk to the bulk power system that must be addressed within 60 days without public disclosure. The determination of a power grid emergency would require the expertise of the Secretary of Energy, in consultation with the Secretary of Homeland Security, Office of Attorney General, and the Director of National Intelligence. In making a determination of a power grid emergency, the Secretary of Energy could consider the existence of the following conditions:

- A known cyber vulnerability exists that may affect the bulk power system.
- A threat actor is determined to have known or suspected intent, requisite resources, and capabilities to carry out the threat with a high likelihood.

- If exploited, the vulnerability would result in significant consequences, including damage to assets and infrastructure, loss of life, and psychological damage.
- The situation presents an imminent risk to the bulk power system.

Any directive should define security performance objectives and metrics for mitigating the identified threat, vulnerability, and/or potential consequences, and specify rules for satisfying the security performance objectives in accordance with the defined metrics within the defined time period of the power grid emergency and require that the fact of the Directive and its contents not be disclosed. The Directive may alternatively be in the form of an alert that notifies owners and operators of a potentially serious cyber situation without specifying mandatory actions that must be taken. Specific methods for compliance shall be left to the discretion of the provider of bulk electric power, provided the security performance objectives are met.

Any directive should notify private sector operators of the bulk power system of the nature of the risk, consistent with the proper handling of classified and restricted information, and direct the operators to investigate, take appropriate and corrective action, and report findings back to FERC within a specified time period, and, if required, direct owners and operators of the bulk power system, through NERC, to develop mitigations, to test and validate such mitigations, and to recommend corrective actions. The Department of Energy could provide technical support in the development, testing, and validation of such mitigation measures.

Conclusions

The scope and nature of security threats and their potential impact on our national security require the ability to act quickly to protect the bulk power system and to protect sensitive information from public disclosure. At the same time, we must continue to build long-term programs that improve information sharing and awareness between the public and private energy sector. The electric system is not the Internet. It is a carefully tended and balanced system that is critical to the Nation and the people. We must continue to strive towards an electric system that can survive an intentional cyber assault with no loss of critical functions.

The following are the Department's recommended courses of action:

- Continue implementation of the "Roadmap to Secure Control Systems for the Energy Sector."
- Study HILF events and conduct cost-benefit analyses of the mitigations

- Continue efforts to improve incident response and information sharing programs.
- As Smart Grid efforts are developed, build into such initiatives, security features designed to anticipate and address cyber security threats.

This concludes my statement Chairman Markey. Thank you for the opportunity to address the committee. I look forward to addressing any questions you or your colleagues may have.

Mr. MARKEY. Thank you, Ms. Hoffman, very much.

Our next witness is Mr. Garry Brown. He is the chairman of the New York State Public Service Commission. Mr. Brown is testifying on behalf of the National Association of Regulatory Utility Commissioners that will henceforth in this committee be referred to as NARUC, which will completely confuse anyone watching on C–SPAN.

So this is your last notice, viewers. It is the National Association of Regulatory Utility Commissioners. So, all 50 States have them. They each decide, kind of, what the electricity and telephone rates are in your State.

Mr. Brown is going to speak for all of them in America. He has 30 years of experience in mastering the arcane language of regulatory law.

And you have 5 minutes, Mr. Brown.

STATEMENT OF GARRY A. BROWN

Mr. BROWN. Good morning, Chairman Markey.

As you said, I am the Chair of Electricity Committee at NARUC.

State regulators take the reliability and security of the bulk power system very seriously. However, as technology changed, new risks and vulnerabilities have emerged. The transition to a smarter, digital, more efficient grid carries with it potential concerns.

Do you want me to talk through it?

Mr. MARKEY. You can continue through.

Mr. BROWN. Thank you.

As Congress considers legislation in this area, it should seek to build on existing——

Mr. MARKEY. When the bells ring, it tells us with two bells that there is a roll call—this won't come off of your time—three bells, that we have a quorum.

When it goes out to six bells and then it goes six bells and then six bells and six bells, you should start running very fast. But that hasn't occurred in my 33 years here. But I just want to notify you that, if it just keeps going through and ringing, that that is not a good thing. But, so far, our reliability counsel up here——

Mr. SHIMKUS. Mr. Chairman, it is worse when there is no power, so you hear no bells.

Mr. MARKEY. So this is maybe the key hearing. Otherwise, we will be reliant upon the same system that my district relied upon in 1775, with Paul Revere riding through and knocking on people's doors and saying, "Get out your gun."

So, anyway, you have 4 minutes and 29 seconds to go, Mr. Brown.

Mr. BROWN. Thank you.

As Congress considers legislation in this area, it should seek to build on existing Federal-State coordination that results in a framework where vulnerabilities to the system are identified, prioritized, and resolved in a timely fashion. Congress needs to distinguish between imminent threats, which require immediate action, and vulnerabilities, which can be resolved more deliberately.

Our first vulnerability focuses on business process systems—e-mail, office equipment, databases, et cetera—that are not unique to

utilities but take on special significance given the utilities' economic importance.

A second vulnerability is more specific to utilities, and that is utility control systems. Supervisory control and data acquisition, or SCADA, systems are already inextricably part of our utility operations and have served to improve the efficiency and reliability of our system operations in every system throughout the country.

Regulatory commissions have begun to probe the cyber-preparedness of utility companies in the realm of smart grid. In concept, the smart grid has the potential to provide improvements in situational awareness, prevention, management, and restoration. In spite of introducing new vulnerabilities, smart grid fundamentally makes the electric system more secure. Still, this technology brings with it new vulnerabilities and new points of access to create intentional disruption, which should be taken extremely seriously.

In each of these areas, steps are being taken to manage risk. The regulated companies we oversee have, through the North American Electric Reliability Corporation, developed good cybersecurity standards. The question of how far that standard extends is not yet clear. NERC's cybersecurity standards are extensive and thorough. Over the past 2 years, electric utilities across the country have requested significant additional staffing and significant additional dollars for NERC's standard compliance activities in their transmission rate case filings at FERC.

The standards already in place are adequate for both physical and cybersecurity. Overextending the applicability of those standards to lower-voltage facilities raises the question how much more we are willing to pay for what may be a marginal increase in cybersecurity.

I would like to share three examples of commissions engaged to ensure companies are meeting their responsibilities.

Since 2005, the Pennsylvania Public Utility Commission has required all jurisdictional utilities to have a written cybersecurity plan to complement their emergency response, each of which are tested on an ongoing basis.

Another State taking action is Missouri. The commission requires all of its utilities to have in place reliability plans and, in May 2009, queried its utilities about steps taken or planned regarding cybersecurity as it relates to company operations. The contacts made highlighted NERC order number 706, which mandates that electric companies adhere to eight standards relative to cybersecurity.

Since 2003, the New York Commission's Office of Utility Security has carried out a regular program of oversight of both physical and cybersecurity practices and procedures of the regulated utility companies in the energy telecommunications and water sectors. Staff of this office is devoted full-time to security audit responsibilities.

Generally, we utilize the existing NERC CIP standards as benchmarks to form our own judgments about the quality of cybersecurity measures in place at the regulated utilities. Staff is adhering to a schedule that calls for visiting each regulated utility company four times a year to audit compliance with some portion of CIP standards, with the goal of measuring compliance with all of the standards at each of the companies over the course of the year.

We have the benefit in New York of a close and effective partnership with our State cybersecurity office. The New York Office of Cybersecurity and Critical Infrastructure Coordination directs efforts to maintain cybersecurity practices within State government agencies. We have established an excellent record for being a prompt and reliable source of information. I have personally been in consultation with CCIC and NERC to consider cyber threats and risks to the smart grid.

I want to get to Federal legislation quickly. NARUC believes Congress should build upon existing Federal-State coordination and result in an environment where vulnerabilities are identified, prioritized, and resolved in a timely fashion. Congress needs to distinguish between imminent threats, which require immediate action, and vulnerabilities, which can be resolved more deliberately.

First, a component of any legislation should be the ability for Federal departments and agencies to have information identifying priority vulnerabilities and imminent threats and how this information is communicated to the various electricity providers, State and Federal law enforcement, and State regulatory authorities.

In normal situations, the electric power industry can protect the reliability and security of the bulk power system without governmental intelligence information. However, in the limited circumstances——

Mr. MARKEY. If you can summarize, Mr. Brown, please.

Mr. BROWN. Yes, I can.

In the limited circumstances when the industry does not need governmental intelligence information on a particular threat or vulnerability, it is critical that such information be timely.

NARUC believes H.R. 2165 takes the best approach to the issues that confront cybersecurity in our Nation's electric system. And we thank Representative Barrow, Chairman Waxman, and Chairman Markey for introducing this legislation. There is a need for Federal leadership on these complex cybersecurity issues.

This concludes my remarks, Mr. Chairman.

[The prepared statement of Mr. Brown follows:]

BEFORE THE
UNITED STATES HOUSE OF REPRESENTATIVES

COMMITTEE ON ENERGY AND COMMERCE,
SUBCOMMITTEE ON ENERGY AND THE ENVIRONMENT

TESTIMONY OF THE HONORABLE GARRY BROWN
CHAIRMAN, NEW YORK STATE PUBLIC SERVICE COMMISSION

ON BEHALF OF THE
NATIONAL ASSOCIATION OF REGULATORY UTILITY COMMISSIONERS

ON

"Protecting the Electric Grid: H.R. 2165, the Bulk Power Systems Protection Act of 2009, and H.R. 2195"

October 27, 2009

National Association of
Regulatory Utility Commissioners
1101 Vermont Ave, N.W., Suite 200
Washington, D.C. 20005
Telephone (202) 898-2200, Facsimile (202) 898-2213
Internet Home Page http://www.naruc.org

Good morning Chairman Markey, and Members of the Subcommittee:

My name is Garry Brown, and I am Chairman of the New York State Public Service Commission (NY PSC). I also serve as Chair of the Electricity Committee of the National Association of Regulatory Utility Commissioners (NARUC), on whose behalf I am testifying here today. I am honored to have the opportunity to appear before you this morning and offer a State perspective on "Cyber Security."

NARUC is a quasi-governmental, non-profit organization founded in 1889. Our membership includes the public utility commissions serving all States and territories. NARUC's mission is to serve the public interest by improving the quality and effectiveness of public utility regulation. Our members regulate the retail rates and services of electric, gas, water, and telephone utilities. We are obligated under the laws of our respective States to assure the establishment and maintenance of such utility services as may be required by the public convenience and necessity and to assure that such services are provided under rates and subject to terms and conditions of service that are just, reasonable and non-discriminatory.

I want to thank you for holding this timely hearing. State regulators take the reliability and security of the bulk-power system very seriously. Through strong federal, State, public, and private partnerships, we have consistently maintained and improved reliability and security of the grid. As times and technologies have changed, new risks

and vulnerabilities have emerged. The transition to a smarter, digital, more efficient grid — while full of promise — carries with it unforeseen concerns and unintended consequences. As Congress considers legislation in this area, it should build on existing federal-State coordination and result in a framework where vulnerabilities to the system are identified, prioritized, and resolved in a timely fashion. Such legislation must distinguish between imminent threats, which require immediate action, and vulnerabilities, which can be resolved more deliberately.

State commissions are old hands at overseeing and ensuring the highest levels of reliability from our nation's utility service providers. Reliable service is the top priority of commissions, even more than affordability and environmental friendliness: if the lights go off, it doesn't matter how cheap or green the electricity is. Our nation's utilities (municipal, cooperative, and investor-owned) have done this country proud in responding to the greatest calamities and catastrophes, quickly and capably restoring power after hurricanes, earthquakes, wildfires, and as my State can attest, acts of terrorism. Commissions understand that preparedness should not focus on response, but should also assure that resilience is built into our infrastructure as a core principle.

As with most sectors of the economy, information systems are rapidly merging with utility systems, potentially heightening the risks of service disruption. Cyber security is an emerging area of risk for our utilities and State Commissions as well, and although it is unique in some respects, this is not the first time our utility systems have faced new reliability threats. Through a strong public-private partnership, we have

overcome past risks, and it is my belief that overall, this merging of information systems into the electric and other utility sectors improves their resilience, reliability and efficiency.

By way of background, State commissions are economic regulators. We have not traditionally had a national security role, either at the State or national level, as this is the province of Emergency Management Agencies, State Policy, and Departments of Homeland Security. However, now the lines defining and separating roles in critical infrastructure protection between the federal government, state agencies, and the private sector owners of critical infrastructure are necessarily overlapping. Cooperation and acceptance of responsibility is a must. With modern threats becoming apparent to us in the last several years, we understand that our traditional responsibility to ensure reliable service must include the need to ensure security. Breaches of security, obviously, can have extremely serious reliability consequences. From my vantage point, State commissions can identify certain key areas of concern about cyber security. The first concern focuses on business process systems — email, office computing, databases, etc. — that are not unique to utilities. In fact, commissions in recent years have improved their own security, along with everyone else, as attacks on these systems become more sophisticated and we become more dependent on them for our operations.

A second vulnerability is more specific to regulated utilities: control systems. Supervisory Control and Data Acquisition (SCADA) systems are already inextricably part of utility operations, and have served to improve the efficiency and reliability of our

system operations in every system throughout the country. In recent years, vulnerabilities to these SCADA systems have been repeatedly highlighted, perhaps most notably through the "Aurora" incident.

Finally, commissions have begun to probe the cyber-preparedness of our utility companies in the realm of smart grid. With tens of billions of dollars in investment on the line, commissions want to know that the investments aren't going to introduce new and unmanaged risks. In concept, the smart grid has the potential to provide many improvements in situational awareness, prevention, management, and restoration. In spite of introducing new vulnerabilities, smart grid fundamentally makes the electric system more secure. Still, this technology brings with it new vulnerabilities and points-of-access to create intentional disruption, which should be taken extremely seriously. "Guns-gates-and-guards" analogs of password protection and "security through obscurity" must be augmented with a framework of maximum system resilience and next-generation safeguards that allow the network to be impregnable, even if devices connected to it are compromised.

In each of these areas, steps are being taken to manage the risk. The regulated companies that we oversee have, through the North American Electric Reliability Corporation, developed standards for cyber security that we believe are a good step in the right direction for SCADA and business process systems. NERC, for example, has adopted a cyber-security standard for the bulk electric system. The question of how far that standard extends (i.e., to what extent it would reach down into the distribution

system) is not yet clear. NERC's cyber security ("CIP") standards are extensive and thorough. Over the past two years, electric utilities across the country have requested significant additional staffing and dollars for CIP standard compliance activities in their transmission rate case filings at FERC. The CIP standards already in place are adequate for both physical and cyber security. However, extending the applicability of those standards to lower voltage facilities raises the question of how much more we are willing to pay for a marginal increase in cyber security. The issue of how much more money should be put into this effort when it is virtually impossible to stop some cyber attacks (e.g., hackers getting into the Pentagon's computer system) needs to be addressed.

Smart grid poses an additional, and particularly thorny, policy issue as well. Through NARUC's collaborative with FERC on smart grid and through other activities, State commissions have also begun to identify key areas to assure that smart grid investments boast the highest, most sophisticated levels of security. Recent federal funding support for smart-grid investments has incentivized the deployment of hardware in advance of the development of standards for cyber security, among other issues. Commissions may be confronted with expenditures on cyber security for which no specific standard has yet been reached. This draws commissions into specific areas of review in order to determine the prudence of expenditures — a review that would be unnecessary if the expenditure would be made in compliance with recognized standards.

Commissions therefore have had to become more expert in their understanding of prudent smart grid and cyber security investments. Because we are not security

regulators, our interest in the area is driven only by our obligation to assure the reliability of service for our ratepayers and the prudence of the costs (including cyber-security spending) that goes into their rates.

Let me give you three examples of activity that commissions have engaged in to ensure that companies are focused on this issue.

Since 2005, the Pennsylvania Public Utility Commission has required all jurisdictional utilities to have a written cyber security plan to complement their emergency response, business continuity and physical security protocols, each of which are tested on an ongoing basis. Earlier this year, the Pennsylvania PUC issued an order on cyber security in reaction to media reports of grid infiltration by international hackers. Pennsylvania also issued a secretarial letter to its utilities encouraging them to be active in the NIST Standards development process by reviewing and commenting on the NIST Framework and the Cyber Security Coordination Task Group documents and to participate in various related working groups.

While Pennsylvania has not done specific audits, investigations or reviews of cyber-security plans on their own, it has incorporated cyber-security review in its management audits process. Pennsylvania performs management and efficiency audits at least once every five years on all electric, gas, and water utilities with over $10 million of plant in service.

Another State taking action is Missouri. Missouri requires all of its utilities to have in place reliability plans, and in May 2009 queried its utilities about steps taken or planned regarding cyber security as it relates to company operations. The Missouri Commission required the utilities to furnish Staff with a verified statement stating if the company is in compliance with NERC Order No. 706 or what actions and how long the company will take to become compliant. The Commission also asked what other organizations, groups, industry groups or other organizations these companies participate with, such as local FBI or State agencies, regarding security issues.

In my own State of New York we are sharing the responsibility for critical infrastructure protection at the Department of Public Service. Since 2003, when it was created, our Office of Utility Security has carried out a regular program of oversight of both physical and cyber security practices and procedures at the regulated utility companies in the energy, telecommunications and water sectors. Staff of this office is devoted full time to this security audit responsibility. Generally, we utilize the existing NERC CIP standards as benchmarks to form our own judgments about the quality of cyber security measures in place at the regulated utilities. Staff is adhering to a schedule that calls for visiting each regulated electric utility company four times a year to audit compliance with some portion of the CIP standards, with the goal of measuring compliance with all of the standards at each company over the course of a year.

We have the benefit in New York of a close and effective partnership with our umbrella State cyber security office. The NYS Office of Cyber Security and Critical

Information Coordination (CSCIC) directs efforts to maintain good cyber security practices within State government agencies. CSCIC also provides cyber threat and vulnerability information externally to several infrastructure sectors, establishing an excellent record for being a prompt and reliable source of such information. We at the Department of Public Service work closely and constantly with both CSCIC and our State Office of Homeland Security on infrastructure protection preparedness. We share information regularly and often through the Governor's Homeland Security Executive Council, and less formal daily interactions. We collaborate to provide joint briefings and notifications to utility company information systems managers regarding cyber threats and countermeasures, and just discovered vulnerabilities.

FEDERAL LEGISLATION

I would now like to briefly address legislation that is currently being considered in the 111th Congress. As I have previously stated in this testimony, NARUC believes that as Congress considers legislation in this area, it should build upon existing federal-State coordination and result in an environment where vulnerabilities to the system are identified, prioritized, and resolved in a timely fashion. Congress needs to distinguish between imminent threats, which require immediate action, and vulnerabilities, which can be resolved more deliberately.

Importantly, any legislation in this area should focus on the ability for federal agencies with information identifying priority vulnerabilities and imminent threats to

communicate with the various electricity providers, State and federal law enforcement entities, and State regulatory authorities. In nearly all situations, the electric power industry can protect the reliability and security of the bulk power system without government intelligence information. However, in the limited circumstances when the industry does need government intelligence information on a particular threat or vulnerability, it is critical that such information is timely and actionable. After receiving this information, the electric power industry can then direct its expert operators and cyber security staff to make the needed adjustments to systems and networks to ensure the reliability and security of the bulk power system.

In short, if the federal government is aware of a vulnerability or threat but does not effectively communicate that information to the utilities, how can they be expected to address these concerns? Additionally, State regulators must be given adequate information so that they are not in a position where they must sign a "blank check" for the mitigation of any federally identified vulnerability, which will then be passed onto ratepayers, along with potential new greenhouse gas mitigation costs.

We believe that neither H.R 2165, introduced by Representative Barrow, and H.R. 2195, introduced by Representative Thompson, or S. 1462 from Senator Bingaman, offer the needed guidance to ensure that the federal entities provide timely and actionable information to the energy providers or State government agencies. Perhaps provisions could be added to establish a process for federal intelligence agencies to provide the requisite security clearance to an employee with responsibility for cyber security. I am

told that there are employees at energy providers and some State agencies that have "secret" level clearance; however in some instances this level would not be adequate.

Second, the scope of legislation should be limited to cyber security on the bulk power system and in emergency situations. If the federal government has actionable intelligence about an imminent threat to the bulk power system, State commissions are ready, willing and able to provide any assistance or issue any complementary orders that may be necessary with regard to similar emergency situations on the distribution systems. In these limited circumstances, when time does not allow for classified industry briefings and development of mitigation measures for a threat or vulnerability, FERC in the United States and the appropriate corresponding authorities in Canada should be the government agencies that direct the electric power industry on the needed emergency actions. These actions should only remain in effect until the threat subsides or upon FERC approval of related NERC reliability standards.

In the United States, Section 215 of the Federal Power Act (Energy Policy Act of 2005) invested FERC with a significant role in bulk power system reliability, and it would be duplicative and inefficient to recreate that responsibility at another agency. It is our opinion that H.R. 2165 is preferable to the other bills in this regard.

Additionally, we recognize that it may be necessary for federal government authorities to intervene, should it have actionable intelligence about an imminent cyber threat that would harm our national security, with regard to distribution assets. In these

instances and in very limited locations federal actions could require certain actions to be taken by the electric power industry. However, we must insist that State commissions or other appropriate State agencies be fully included from beginning to end of the emergency situation. We would suggest that language be included in H.R. 2165 to address and limit the circumstances where this could occur.

In total, NARUC believes that H.R. 2165 takes the best approach to the issues that confront cyber security on our nation's electric system and we thank Representative Barrow, Chairman Waxman, and you Chairman Markey for introducing this legislation.

SPECIFIC SUBCOMMITTEE QUESTIONS

Mr. Chairman, in your invitation you requested that in my testimony I provide answers to seven questions you posed. I have alluded to some of them previously, and will attempt to provide general responses here:

1. What measures, if any, are state public utilities commissions taking to protect the electric grid against cyber security, EMP, or other vulnerabilities to and threats from malicious acts?

As regulators of investor-owned utilities, and, in some instances, municipal and co-op utilities, State commissions broadly become involved in their capacity to oversee reliable service and to ensure prudent expenditures by the electric utility companies.

Ensuring reliable service means holding utilities to high levels of performance in the face of all hazards. Commissions require utilities to comply with reliability standards and to possess emergency preparedness plans that minimize or eliminate the possibility of events with varying probabilities and consequences (ranging from hurricanes to insider acts). Moreover, commissions approve the prudence of expenditures on all activities, including critical infrastructure protection, via the rate case process.

Some commission staffs retain experts on security and critical infrastructure protection. The Public Utilities Commission of Ohio, the New Jersey Board of Public Utilities and the Michigan Public Service Commission are examples of commissions that have been integrated into their Governors' Homeland Security advisory infrastructure. Also, Colorado, New York and Texas have specific staffs detailed to this issue. Even when staff are not been designated with a security focus, NARUC's Committee on Critical Infrastructure has members from most States participating and staying abreast of national trends, issues, and best practices. This committee regularly educates and engages members in tabletop exercises, workshops, and dialogues on topics ranging from hurricanes to copper theft. Cyber security has been a core discussion topic for the past three years.

Specific to cyber security, commissions vary in their approaches. Some, such as New York, Texas, and Oregon, have or are acquiring specific expertise in cyber security. Others more indirectly rely on CIP standards compliance or reliability standards adherence to ensure that this area is addressed.

2. What gaps or limitations, if any, are there in the existing process and standards under section 215 of the Federal Power Act for ensuring that the electric grid is adequately protected against cyber security, EMP, or other vulnerabilities to and threats from malicious acts?

Through strong federal, State, public, and private partnerships, we have consistently maintained and improved reliability and security of the grid. As times and technologies have changed, new risks and vulnerabilities have emerged. The transition to a smarter, digital, more efficient grid — while full of promise — carries with it unforeseen concerns and unintended consequences. As Congress considers legislation in this area, it should build upon the existing federal-State coordination and result in an environment where vulnerabilities to the system are identified, prioritized, and resolved in a timely fashion. Congress needs to distinguish between imminent threats, which require immediate action, and vulnerabilities, which can be resolved more deliberately.

3. What new federal authority, if any, is needed to protect the grid against such vulnerabilities and/or threats – whether in the form of emergency response authority or standard-setting authority? If new authority is needed, what federal agency or agencies, or other entity (such as the North American Electric Reliability Corporation) should be tasked with such authority and how should it be structured?

NERC has adopted a cyber-security standard for the bulk electric system. NERC's cyber security ("CIP") standards are extensive and thorough. Over the past two years, electric utilities across the country have requested significant additional staffing and dollars for CIP standard compliance activities in their transmission rate case filings at FERC. The CIP standards already in place are adequate for both physical and cyber security. The question of how far that standard extends (i.e., to what extent it would reach down into the distribution system) is not yet clear and needs to be better defined. Extending the applicability of those standards to lower voltage facilities raises the question of how much more we are willing to pay for a marginal increase in cyber security. The issue of how much more money should be put into this effort when it appears virtually impossible to stop some cyber-attacks (e.g., hackers getting into the Pentagon's computer system) needs to be addressed.

4. If new federal authority is needed in this area, should it extend only to cyber security vulnerabilities and/or threats, or should it also address physical vulnerabilities and/or threats, or some subset thereof, such as vulnerabilities and/or threats specifically related to EMP or large transformers?

Cyber security may pose a new paradigm for some because of the ability of a cyber attack to be geographically remote from the affected area. As such where near-term threats are identified it may be relevant to introduce emergency authority by federal authorities.

For large transformers, programs are already being put into place, such as the Spare Transformer Exchange Program (STEP), the costs of which have already been approved by commissions in every participating footprint. No further federal authority is warranted in this area.

With regards to EMP, it is appropriate for the federal government to weigh the probability and consequence of this vulnerability, as without such analysis there is no basis for Federal authority. In the interim, EMP should be weighed among other vulnerabilities, and decisions made in circumstances that consider the cost-effectiveness of mitigation of this vulnerability against cost effectiveness for addressing a range of hazards. It is not an appropriate area for new federal authority unless a real threat (i.e., a new significant probability of occurrence) is identified, as there is a clear lack of authority on the part of other decision makers to manage this vulnerability.

5. If new federal authority is needed in this area, should it extend beyond the bulk power system to distribution system assets and/or Alaska, Hawaii, and U.S. territories? If any such extension beyond the bulk power system is warranted, should such extension be limited to some subset of "critical" assets, such as those serving defense facilities or major metropolitan areas? If so, how should such "critical" assets be defined?

With regards to cyber security, Alaska and Hawaii may also be subject to geographically dislocated attacks, and therefore emergency basis federal authority may

well be warranted. With regards to other physical and emerging threats, such as EMP, no such authority is relevant.

The question of cogently defining "critical assets" has eluded experts and specialists for a decade — it is a moving target dependent on circumstance. Most utility assets are critical at some level to some operation or constituency. Identification of essential assets is a routine element of utility and transmission operator activities, with hundreds of multiple failure level scenarios being modeled in real-time. The existing standards and practices that govern the level of preparedness by these operators is adequate and no new authority is needed unless a near-term threat, of significant consequence and probability, is identified

6. If new federal authority is needed in this area, how should treatment of sensitive information be addressed?

State commissions continue to deal with the treatment of sensitive information. While commercially sensitive and security sensitive information must be protected from FOIA and public release, a real risk emerges when those holding the information fail to connect decision-makers with the information that they need to take action. A partnership approach is warranted where any new authority is granted

7. If new federal authority is needed in this area, how should utilities' recovery of costs for compliance with federal directives be addressed, if at all?

Recovery of costs need not be addressed in this legislation. Currently, State rate regulated utilities have the ability to recover federally mandated costs, for example the Nuclear Waste Fund fees and acid rain mitigation costs. We do not see the necessity for different cost recovery treatment in this legislation.

CONCLUSION

A long-standing mission of the State public utility commissions is to ensure the physical viability of the utility plant under their supervision. A less traditional responsibility, cyber security and information systems standards and development, is increasingly thrust into the mix, yet this newer responsibility clearly envelops a broader range of industries and specific expertise. Utility regulators recognize the dependence of sound cyber security practices and cyber reporting on sound construction practices and utility-outage reporting, and visa versa.

A concern that I wish to leave with you for consideration is that protocols intended to distinguish between disruptions to critical infrastructure related to cyber events and those related to physical events, e.g., a denial-of-service attack as opposed to a fiber-optic cable failure, have not kept up with the fast-emerging nature of cyber threats. Such protocols are easier to craft than to implement. The first evidence of disruption is the disruption itself, and such events do not often present themselves with the root cause clearly visible.

In the critical "golden hours" after a possible new developing threat is detected, or immediately following an event, it may not always be clear what is actually happening or why. For this reason, close coordination between the utility sector and the cyber sector is essential to the response. As the State public utility commissions have traditionally served as the gateway to the utility sector and have their own independent core of expertise and relationships key to understanding in real-time events affecting that plant, close coordination among the operators of our cyber networks, the federal government, and State homeland security partners, including utility commissions, is essential.

Mr. Chairman and members of the Subcommittee, this concludes my testimony. State public service commissions take the issues of cyber security and reliability seriously. We believe a federal-State, public-private partnership is essential to meeting these challenges over the long term. I am now happy to answer any questions from the Subcommittee. Thank you.

Mr. MARKEY. Thank you, Mr. Brown, very much.

Our next witness is Mr. David Cook. He is the vice president and general counsel of the North American Electric Reliability Council, or NERC. In this role, Mr. Cook helps to lead the development of mandatory and enforceable reliability standards for the electric grid.

Prior to joining NERC in 1999, Mr. Cook worked for 10 years as deputy general counsel of the Federal Energy Regulatory Commission.

So, again, just for our audience, Mr. Cook is speaking for NERC, which is the private sector. Mr. Brown is speaking for NARUC, which are the State regulators. And the first two witnesses speak for the Federal Government, and that would be the Department of Energy, which I think everyone knows, and the FERC, Federal Energy Regulatory Commission.

We have FERC and NERC, and it does get confusing to people, oK, but it is Federal Government, State government, and now the private sector.

Mr. Cook, whenever you are ready, please begin.

STATEMENT OF DAVID N. COOK

Mr. COOK. Thank you, Mr. Chairman and members of the subcommittee.

NERC's overall mission is to ensure the reliability of the bulk power system in North America. Cybersecurity is an important component of that mission. The challenges the grid faces from cybersecurity threats, however, are different from other reliability concerns.

Digital technology changes frequently, and novel potential threats can arise very quickly, requiring rapid and often confidential responses. Threats can arise virtually any time and anywhere across the vast array of communicating devices on the grid. Moreover, cybersecurity threats are more likely to be driven by intentional manipulation of devices rather than weather-related or operational events that regularly occur on the system.

All of these characteristics set cybersecurity apart from other reliability concerns. For these reasons, NERC believes that the U.S. Government needs additional emergency authority to address specific imminent cybersecurity threats.

As the international regulatory authority for the reliability of the bulk power system, NERC is responsible for developing reliability standards applicable to all users, owners, and operators of the system. The standard-setting process brings together NERC and industry and security experts from the United States and Canada to develop standards that must apply to the international grid.

Developing long-term standards that apply to more than 1,800 diverse entities that own and operate the bulk power system is a complex undertaking. Standards must apply equally to companies with thousands of employees and those with only 20. Additionally, the standards must do no harm.

NERC recognizes that, while the standards in place today provide a sound starting point, they should be and are being improved. NERC is also working in a number of areas to make available the kinds of information that will help the industry better secure crit-

ical assets from advanced well-resourced threats and other known cybersecurity activity on an ongoing basis.

In its role as the electricity-sector information sharing and analysis center, NERC analyzes and disseminates threat information and warnings to the electricity industry in the form of voluntary advisories, recommendations to industry, and essential action notifications.

NERC's preparedness and awareness efforts are necessary but not sufficient to protect the system against imminent specific cybersecurity threats. The principal gap that NERC sees in the current law is that the Federal Government lacks sufficient authority to address an imminent and specific cybersecurity threat. Both H.R. 2165 and H.R. 2195 address that gap.

NERC believes the authority to act in such emergencies should be assigned to a single Federal agency. The legislation should also assure coordination between the Federal agency with that authority and appropriate officials in Canada and Mexico. H.R. 2165 contains important provisions that require such consultation, while H.R. 2195 contains no specific provisions in this area.

The jurisdiction provided by H.R. 2195 would go beyond the scope of existing Section 215 to cover distribution system assets. 2165 would limit its scope to the existing Section 215.

While physical threats are also a concern, NERC believes addressing the present gap and authority to address specific imminent cybersecurity threats is the highest legislative priority at this time.

One of the greatest challenges the industry faces in dealing effectively with the threats we have been discussing is the limited amount of concrete technical information coming from government agencies. Much of the information about threats is classified or otherwise subject to restrictions on disclosure.

Without more specific information being appropriately made available to asset owners, they are unable to determine whether particular cybersecurity concerns exist on their systems or develop appropriate mitigation strategies. A mechanism, therefore, is needed to validate the existence of such threats and ensure information is appropriately conveyed.

Over the past year, NERC has worked to facilitate this information sharing and stands ready to support further efforts in this area. Both H.R. 2165 and H.R. 2195 contain provisions to address this problem.

To conclude, NERC, the electric industry, and the governments of North America share a mutual goal of ensuring that threats to the reliability of the bulk power system, especially cybersecurity threats, are clearly understood and effectively mitigated. NERC fully supports legislative efforts to provide the Federal Government with emergency authority to address imminent cybersecurity threats as quickly as possible.

Moving forward, NERC is committed to complementing Federal authority to address cybersecurity challenges, regardless of the form that legislation may take.

Thank you.

[The prepared statement of Mr. Cook follows:]

TESTIMONY OF DAVID N. COOK
VICE PRESIDENT AND GENERAL COUNSEL
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

BEFORE THE
SUBCOMMITTEE ON ENERGY AND ENVIRONMENT
COMMITTEE ON ENERGY AND COMMERCE
U.S. HOUSE OF REPRESENTATIVES

Hearing on

PROTECTING THE ELECTRIC GRID: H.R. 2165, THE BULK POWER SYSTEM PROTECTION ACT OF 2009, AND H.R. 2195

October 27, 2009

INTRODUCTION

The North American Electric Reliability Corporation ("NERC") takes most seriously its role in ensuring the cyber security of the electric grid. Working with stakeholders, NERC's overall mission is to ensure the reliability of the Bulk Power System in North America. Cyber security is clearly one component of that mission. The challenges the grid faces from cyber security threats, however, are different from other reliability concerns. Unlike traditional concerns (such as vegetation management on transmission line right-of-ways) for which there is significant operating experience, digital technology changes frequently and novel potential threats can arise very quickly, requiring rapid and often confidential responses. Threats can arise virtually anytime and anywhere across the vast array of communicating devices on the grid – Supervisory Control and Data Acquisition (SCADA), control rooms, power plants, substations, relays, meters, some transformers, capacitor bank controllers, to name just a few – and the systems to which those devices are connected. Cyber security threats are also more likely

to be driven by intentional manipulation of devices as opposed to operational events on the Bulk Power System.

All of these characteristics clearly set cyber security apart from other reliability concerns. Where there is an identified, immediate threat, a different approach is required – one that allows for more expedient and confidential treatment of critical information, rapid threat analysis, and specific, directed action when necessary. For these reasons, NERC believes that the U.S. government needs additional emergency authority to address specific, imminent cyber security threats. With immediate emergency authority in the hands of government, NERC would be better positioned to develop and implement longer-term cyber security and critical infrastructure protection Reliability Standards.

My testimony today will focus on the process and standards in place under Section 215 of the Federal Power Act ("FPA") for ensuring that the electric grid is adequately protected against cyber and other vulnerabilities and threats. I will also offer NERC's views on elements of the pending legislation, including H.R. 2165 and H.R. 2195, to establish additional authorities to address cyber security threats to the Bulk Power System.

I. ROLE OF NERC STANDARDS IN PROTECTING THE BULK POWER SYSTEM FROM CYBER ATTACK

As the international regulatory authority for the reliability of the Bulk Power System in North America, NERC is responsible for developing Reliability Standards applicable to all users, owners and operators of the Bulk Power System. In the United States, NERC was certified as the Electric Reliability Organization by the Federal Energy Regulatory Commission ("FERC") under Section 215 of the FPA in July 2006. NERC is similarly recognized in much of Canada, with the goal of ensuring that the entire interconnected North American power system operates from a single platform of sound Reliability Standards. NERC's over 100 Reliability Standards cover reliability issues ranging from vegetation management to system operator training to modeling of the Bulk Power System.

In January 2008, FERC issued Order No. 706, approving eight mandatory Reliability Standards for Critical Infrastructure Protection ("CIP Reliability Standards") developed by NERC through its ANSI-accredited standards development process.[1] These standards set forth specific requirements that are binding on users, owners and operators of the Bulk Power System to safeguard critical cyber assets.

The CIP Reliability Standards are comprised of roughly forty specific requirements designed to lay a solid foundation of sound security practices that, if properly implemented, will help develop the capabilities needed to secure critical

[1] *Mandatory Reliability Standards for Critical Infrastructure Protection,* Order No. 706, 122 FERC ¶ 61,040, *reh'g denied,* Order No. 706-A, 123 FERC ¶ 61,174 (2008).

infrastructure from cyber security threats. Audits of compliance with certain requirements included in the standards began on July 1, 2009.

NERC recognizes, however, that while the standards in place today provide a sound starting point, they should be improved. NERC has worked with industry, consumer representatives and regulators to strengthen the CIP Reliability Standards both in the short term by means of an initial six-month revision phase, and the longer-term, through a concurrent revision phase. The initial revisions to the CIP Reliability Standards were approved by FERC as Version 2 of the CIP Reliability Standards on September 30, 2009.[2] These standards will become effective on April 1, 2010. Work to further strengthen the cyber standards is underway as phase two revisions continue.

One of the areas that must be addressed in these revisions was the subject of an April 7, 2009 letter from NERC Chief Security Officer Michael Assante to industry stakeholders. The letter addressed the identification of Critical Assets and associated Critical Cyber Assets that support the reliable operation of the Bulk Power System, as required by NERC Reliability Standard CIP-002-1.[3] In the letter, Mr. Assante called on users, owners, and operators of the Bulk Power System to take a fresh look at current risk-based assessment models to ensure they appropriately account for new considerations specific to cyber security, such as the need to consider misuse of a cyber asset, not simply the loss of such an asset.

---

[2] *North American Electric Reliability Corp.*, 128 FERC ¶ 61,291 (2009) (Order Approving Revised Reliability Standards for Critical Infrastructure Protection and Requiring Compliance Filing).

[3] The letter is available from the NERC website: http://www.nerc.com/fileUploads/File/News/CIP-002-Identification-Letter-040709.pdf.

The letter demonstrates NERC's focus on addressing a critical element of the cyber security challenge: the educational learning curve and resulting compliance-related challenges that must be addressed to improve the cyber security of the Bulk Power System. Ensuring that each of the approximately 1800 entities that own and operate components of the Bulk Power System understands cyber security and the efforts needed to adequately protect the security of the Bulk Power System has been a priority for NERC. The standards development process itself has contributed a great deal to raising the profile and priority of cyber security within the electric sector. Other educational efforts currently underway include a series of webinars on compliance with the CIP Reliability Standards and regular communication with industry.

Initial results from the most recent CIP Reliability Standards implementation survey indicate that more work is needed with industry to ensure that Critical Assets are being appropriately identified as such. For example, approximately 26 percent of generation facilities in the United States reported to NERC are presently identified by industry as Critical Assets. The specific data is a significant cause for concern regarding the current implementation of the CIP Reliability Standards for certain assets and indicates progress for others. NERC is presently engaged in further evaluating the data received and will be working with stakeholders to develop an action plan to address the issue over the coming weeks.

II. ADDRESSING IMMINENT AND SPECIFIC CYBER SECURITY THREATS

At NERC, we are working in a number of areas to provide or assist in the provision of the kinds of information that will help the industry better secure critical assets from advanced, well-resourced threats and other known cyber activity on an ongoing basis. In its role as the Electricity Sector Information Sharing and Analysis Center (ES-ISAC),[4] NERC analyzes and disseminates threat information and warnings to the electricity industry in the form of Advisories, Recommendations to Industry, and Essential Action Notifications. Alerts issued through this mechanism are not mandatory and cannot require an entity to perform tasks recommended or advised in the alert. NERC has significantly improved the alerts system over the past year and continues improvements through the development of a secure alerting portal, currently in the pre-commissioning user validation phase.

Through the alerts system, NERC is able to provide timely, critical reliability information to nearly 5,000 security and grid operations professionals within minutes, and has demonstrated success by conducting training and using the system to send alerts, record acknowledgements and receive responses within several days. NERC has issued twelve such alerts in 2009, with its most recent "recommendation" receiving a strong 94 percent response rate.

[4] The ES-ISAC has been operated by NERC since it was formed in 2001. The ES-ISAC was created as a result of action by the U.S. Department of Energy in response to Presidential Decision Directive 63 issued in 1998. The ES-ISAC works with the electricity industry to identify and mitigate cyber vulnerabilities by providing information, recommending mitigation measures, and following up to monitor implementation of recommended measures. NERC, in its capacity as the ES-ISAC, also has a related role in cyber and physical security issues associated with all electric facilities operated in the United States.

Preparedness and awareness efforts like the standards and alerts discussed above are necessary, but not sufficient, to protect the system against specific and imminent cyber threats. NERC firmly believes that that in the case of an imminent cyber security threat, authority to direct action should be vested in the Federal government in the United States. NERC supports legislation that would give an agency or department of the Federal government necessary authority to take action in the face of specific and imminent cyber threats.

III. COMMENTS ON PENDING LEGISLATION

Single Federal agency with authority to address imminent threats: Both H.R. 2165 and H.R. 2195 address the principal gap that NERC sees in the current law: the Federal government lacks sufficient authority to act to address an imminent and specific cyber security threat to the critical infrastructure of the United States. NERC believes that authority to act in such emergencies should be assigned to a single Federal agency. H.R. 2165 does this by giving FERC authority to address both certain existing cyber security threats, through interim measures to be issued within 120 days of enactment as necessary, and future emergencies involving imminent cyber security threats (proposed FPA Section 215A(b) and (c)). H.R. 2195 also assigns responsibility to FERC to establish both 1) interim measures that would supplement, replace or modify cyber security Reliability Standards that FERC finds to be inadequate to address known vulnerabilities (under proposed FPA 224B), and 2) rules or orders "necessary" to protect critical electric infrastructure against vulnerabilities or threats identified by the Department of Homeland Security, including emergency orders to protect against an

imminent threat or vulnerability issued without notice or hearing (through proposed FPA 224(c)). In contrast, S. 1462, the American Clean Energy Leadership Act, as reported by the Senate Energy Committee vests authority to act in both the Commission and the Department of Energy ("DOE"), creating potentially competing emergency authorities in both the Secretary of Energy and FERC.

Preservation of the FPA Section 215 Standards Development and Approval Process: The NERC standard-setting process brings together industry and security experts to develop standards that must apply to the international, interconnected grid. Developing long-term standards that apply to the more than 1800 diverse entities that own and operate the Bulk Power System is a complex undertaking. Standards must apply equally to companies with thousands of employees and to those with only twenty. Additionally, the standards must not do harm. They must take into account unique component configurations and operational procedures that differ widely across the grid. Given our extensive experience in standards development, NERC believes the level of expertise needed to create standards that achieve security objectives and ensure reliability can be found within the industry itself. Setting long-term cyber security Reliability Standards should not be done without notice or opportunity to be heard, as valid technical feasibility concerns do exist and must be considered so that adherence to mandatory requirements in one area does not negatively impact other aspects of reliability. NERC has strong concerns regarding the tradeoffs that could be made between compliance-based decisions and those that might otherwise be in the best interests of system reliability. These concerns are also relevant for interim measures. Coordination with a

defined group of industry experts may provide an appropriate mechanism to evaluate proposed measures and identify concerns from a reliability perspective.

H.R. 2165 contains provisions to harmonize the new FERC authorities with the Reliability Standards development process. H.R. 2165 expressly provides that interim measures or actions to address existing cyber security threats are to be replaced by standards developed, approved and implemented under FPA Section 215 (proposed Section 215A(b)(2)). The legislation also specifies when interim measures are to be discontinued, including when a Reliability Standard is developed and implemented pursuant to FPA Section 215 to address the identified threat (proposed Section 215A(d)(2)). FERC orders for emergency measures or actions to protect Bulk Power System reliability against an imminent cyber security threat determined to exist by the President also are to be discontinued upon, among other things, the development and implementation of a reliability standard to address the identified threat (proposed Section 215A(e)(3)).

H.R. 2195 limits the duration of emergency orders issued by FERC without prior notice or hearing (proposed Section 224(d)), but does not otherwise provide that such rules or orders are to be replaced by Reliability Standards under FPA Section 215. Under proposed Section 224B(a)(1), interim measures to protect against known cyber vulnerabilities could replace or modify Reliability Standards established under FPA Section 215. While H.R. 2195 provides that such interim measures "may" be replaced by standards developed and approved under FPA Section 215 (proposed Section 224B(a)(2)), there is no requirement to do so.

S. 1462 would give FERC authority to establish standards to address not only emergencies, but any cyber security vulnerability, defined as a weakness or flaw in the design or operation of any programmable electronic device or communication network that exposes critical electric infrastructure to a cyber security threat. In this way, the legislation would authorize FERC to adopt rules or orders without notice or hearing, and supplant Section 215 with respect to establishing cyber security standards in the first instance.

Coordination with Canada and Mexico: Recognizing the international nature of the North American electric grid, the legislation should assure coordination between the Federal agency with authority to address imminent cyber security threats and appropriate officials in Canada and Mexico. H.R. 2165 contains important provisions that require consultation with Canada and Mexico before the establishment of interim measures to address existing cyber security threats (proposed Section 215A(b)(1)), as well as consultation to the extent practicable before emergency orders are issued (proposed Section 215A(c)(2)). H.R 2195 contains no specific provisions in this area.
The provisions of S. 1462 dealing with the emergency authority of the Secretary of Energy encourage consultation and coordination with Canada and Mexico, but there is no corresponding requirement imposed on FERC.

Focus on the Bulk Power System: Certain aspects of the pending legislation go beyond the scope of Section 215, which specifically limits standard-setting authority to apply only to users, owners, and operators of the Bulk Power System. H.R. 2195 provides that FERC rules or orders to protect against known cyber vulnerabilities or

threats may require any "owner, user or operator of critical electric infrastructure in the United States" to develop a plan to address cyber vulnerabilities identified by FERC and to submit the plan to FERC for approval (proposed Section 224B(b)). The term "critical electric infrastructure" is defined expansively as "systems and assets, whether physical or cyber used for the generation, transmission, distribution, or metering of electric energy that, in the determination of the Commission, in consultation with the Secretary of Homeland Security and other national security agencies, are so vital to the United States that the incapacity or destruction of such systems and assets, either alone or in combination with the failure of other assets, would cause significant harm to the security, national or regional economic security, or national or regional public health or safety." (Proposed Section 224(a).) The potential inclusion of distribution system assets represents an expansion of the jurisdiction under FPA Section 215, which applies to the Bulk Power System only. Similarly, S. 1462 would extend jurisdiction for purposes of cybersecurity to any entity that owns, controls, or operates systems and assets, whether physical or virtual, used for the generation, transmission, or distribution of electric energy affecting interstate commerce. The authorities to be established under H.R. 2165 would operate consistently with the current jurisdiction under FPA Section 215.

At the time Congress adopted Section 215 of the FPA providing for mandatory and enforceable Reliability Standards, it carefully chose the scope of jurisdiction it was granting, based on the nature of the risk and the international nature of the interconnected grid. This authority places appropriate focus on the reliability of the Bulk Power System, as outages and disturbances on the bulk system have the potential for far greater impact

than those on distribution systems. Congress should again weigh the benefits and risks of broader jurisdiction as it considers any grant of additional authority.

Physical vulnerabilities/threats: NERC believes addressing the present gap in authority to address specific, imminent cyber security threats is the highest legislative priority at this time. Authorities and agencies already exist to deal with risks to physical assets, including local and state police, the Federal Bureau of Investigation, and the Departments of Defense and Homeland Security.

EMP: In partnership with the DOE, NERC has recently begun an effort to assess "high impact, low frequency" risks – or, more accurately, those risks whose likelihood of occurrence is uncertain relative to other threats, but that could significantly impact the system were they to occur. Officially launched on July 2, the effort is a culmination of high-level discussions between leadership at NERC and DOE. NERC and DOE will host a closed, invitation-only workshop on November 9-10 to examine the potential impacts of these events on the Bulk Power System. The group will focus on influenza pandemic, geomagnetic disturbances, coordinated cyber and physical attacks, and electromagnetic pulse events. Recommendations from the workshop will be used to drive needed coordination, research, development, and investment.

Treatment of sensitive information: Without more specific information being appropriately made available to asset owners, they are unable to determine whether particular cyber security concerns exist on their systems or develop appropriate mitigation strategies. A mechanism therefore is needed to validate the existence of such

threats and ensure information is appropriately conveyed to and understood by asset owners and operators in order to mitigate or avert cyber vulnerabilities.

All of the pending legislation contains provisions to address the need to provide information on cybersecurity threats that users, owners, and operators require to understand the nature of threats to the Bulk Power System and appropriate responses. H.R. 2165 provides for a new category of "sensitive cyber security information," which would consist of unclassified information that specifically discusses cyber security threats, vulnerabilities, mitigation plans or security procedures (proposed Section 215A(f)(1)(B)). FERC would be required to promulgate rules to provide for the release of such information to users, owners and operators in order to enable them to comply with Commission rules, orders or measures to respond to cyber threats (proposed Section 215A(f)(2)). H.R. 2195 makes the provisions of Section 214 of the Homeland Security Act of 2002, which among other things provide for procedures for the issuance of notices and warnings related to the protection of critical infrastructure and protected systems in a manner that prevents the public disclosure of critical infrastructure information, applicable to critical electric infrastructure information submitted to FERC (proposed Section 224(f)). Concerns remain over the sharing of critical infrastructure information, both at the state level and between federal entities and NERC. These issues should be addressed to ensure information is adequately protected. S. 1462 requires DOE/FERC to establish procedures to release critical infrastructure information to any entity that owns, controls, or operates critical electric infrastructure to enable them to implement rules/orders of DOE/FERC.

Such provisions may help bridge the information gap that today limits understanding of and potentially responses to cybersecurity threats and vulnerabilities.

CONCLUSION

NERC, the electric industry, and the governments of North America share a mutual goal of ensuring that threats to the reliability of the Bulk Power System, especially cyber security threats, are clearly understood and effectively mitigated. NERC believes the highest priority gap in the nation's cyber security protection is the lack of emergency authority, and all of the pending legislative proposals address this gap.

NERC appreciates the magnitude and priority of this issue and fully supports legislative efforts to address this gap in authority as quickly as possible. Moving forward, NERC is committed to complementing Federal authority to address cyber security challenges, regardless of the form it may take.

Mr. MARKEY. Thank you, Mr. Cook, very much.

And our final witness is Mr. John DiStasio. He is general manager and CEO of the Sacramento Municipal Utility District, or SMUD; henceforth called "SMUD" for our hearing purposes.

So we will have SMUD, NERC, NARUC, DOE, and FERC. Good luck, C–SPAN viewers, in this hearing.

He will be discussing bulk power as it is differentiated from a distribution system and how we can coordinate.

So welcome, Mr. DiStasio. Whenever you are ready, please begin.

Mr. MARKEY. And you can see why we should legislate in this area. You can see how it could escape a lot of attention from Congress, in terms of the security of the system.

Welcome, Mr. DiStasio. Whenever you are ready, please begin.

STATEMENT OF JOHN DISTASIO

Mr. DISTASIO. Thank you, Chairman Markey, members of the subcommittee. I appreciate the opportunity to explain how the electric industry is addressing cybersecurity challenges and to support narrowly targeted legislation to enhance those efforts.

SMUD supplies electricity to California's capital region. We serve a population of 1.4 million people. We operate 473 miles of transmission lines but nearly 10,000 miles of distribution lines. Our customers include the State of California, the county of Sacramento, companies such as Intel, and other customers critical to public welfare and our local economy.

SMUD is a member of the American Public Power Association, APPA, and the Large Public Power Council, LPPC. They are part of a larger coalition of electricity stakeholders that have been working together on cybersecurity issues for the last 2 years.

The industry coalition includes investors, cooperatively and publicly owned utilities, utility generators, independent generators, Canadian utilities, large industrial consumers, and State PUCs. We often have very different views on policy issues facing our industry, but on the issue of cybersecurity we have been working together to help develop NERC's reliability standards for critical infrastructure protection and, more recently, to identify areas where additional legislation may be needed.

APPA, LPPC, NARUC, the Canadian Electric Association, the Edison Electric Institute, the Electricity Consumers Resource Council, the Electric Power Supply Association, the National Rural Electric Cooperative Association, and the Transmission Access Policy Study Group all support carefully crafted specific legislation to deal with the discrete issue of cybersecurity.

We understand the seriousness of this issue, and we know we need to deal with it. It is in the industry's best interest to protect against cyber attacks. When the lights go out for whatever reasons, we are the ones held responsible. If they do go out, we want to bring them back on as quickly as possible and to minimize potential risk to health, safety, and property and to minimize any adverse impacts to the public.

At the same time, our industry is facing additional regulatory requirements in a number of areas, which all translate to increased costs for our consumers. Therefore, we must use our dollars and workforce wisely to address cybersecurity threats and

vulnerabilities that are most likely to occur and have the greatest potential impact.

We need close collaboration between government and industry participants, rather than finger-pointing. Therefore, any cybersecurity legislation Congress adopts should continue the strong industry partnership with government agencies in the United States and Canada.

The interconnected North American electric power industry and NERC work closely with the Department of Homeland Security, DOE, FERC, and Canadian authorities. New legislation should be built on this strong foundation.

We support continued participation in NERC's industry based and FERC-approved standards development process. NERC and the industry have committed significant resources to develop revised and new security standards. We have committed some of our scarcest resources, our subject matter experts in cybersecurity and system operations, to help develop second-generation draft standards.

And it should be limited to the realm of cybersecurity. Some would prefer to include new legislation, other national security threats as well as cyber threats. SMUD and the industry coalition believe that other government entities, both State and Federal, have more direct responsibilities for national security.

The electric utility industry addresses physical threats through communication with local, State, and Federal law enforcement agencies and through our own security measures. SMUD has established a strong and long-term partnership and communication with the FBI, Sacramento County Sheriff's Department, El Dorado County Sheriff's Department, and the Sacramento Police Department.

SMUD and the industry coalition support H.R. 2165. This bill sets out a process for the Federal Government to interact with the industry in a cybersecurity emergency but does not disrupt the existing reliability regime set out in section 215.

Specifically, the bill provides narrowly targeted authority for FERC to issue emergency orders in response to imminent cybersecurity threat to the bulk power system, specific authority for FERC to issue orders that address the AURORA vulnerability, improved communication flows of timely and actionable information from government to industry, and enhanced responsibility for us to share critical energy infrastructure information, enhanced authority for the electric power industry to protect and keep critical energy infrastructure information confidential and nonpublic and be limited to the bulk power system.

With that, I will conclude my remarks, as time is out. Thank you.

[The prepared statement of Mr. DiStasio follows:]

Statement

Of the

SACRAMENTO MUNICIPAL UTILITY DISTRICT

For the

HOUSE ENERGY AND ENVIRONMENT SUBCOMMITTEE'S

Hearing Entitled "Protecting the Electric Grid: H.R. 2165, the Bulk Power System Protection Act of 2009, and H.R. 2195"

October 27, 2009

Introduction

The Sacramento Municipal Utility District (SMUD) appreciates the opportunity to provide the following testimony for the hearing entitled "Protecting the Electric Grid: H.R. 2165, the Bulk Power System Protection Act of 2009, and H.R. 2195." I am John DiStasio, General Manager and CEO of SMUD.

SMUD has been supplying electricity to California's capital region since 1946. SMUD serves a population of 1.4 million and has 473 miles of transmission lines and 9,784 miles of distribution lines crossing its service territory of 900 square miles. SMUD's 594,595 residential and business customers include such large accounts as the State of California, the County of Sacramento and Intel. A number of SMUD's customers – including the State of California, Regional Sanitation and local hospitals – are critical to public welfare and economic security.

SMUD is a member of the American Public Power Association (APPA) and the Large Public Power Council (LPPC), both of which are part of a larger coalition of electricity stakeholders that have been working together on the cyber security issue in the legislative arena for the last two years and on grid reliability issues for decades.

The associations in our industry coalition represent a broad variety of stakeholder interests, including investor-owned, cooperatively-owned and publicly-owned utilities, independent generators, Canadian utilities, large industrial consumers, and state public utility commissions. (Although the Subcommittee has invited the National Association of Regulatory Utility Commissioners (NARUC) to testify separately, it is important to note that they are also a part of this broad industry coalition.) For legitimate reasons, we usually have very different views on the policy issues facing our industry. On the issue of protection of the bulk power system from cyber security threats and addressing cyber security vulnerabilities, however, we have been working together in recent years to help develop the North American Electric Reliability Corporation's (NERC) reliability standards for critical infrastructure protection and more recently, in the last two years, on identifying areas where additional legislation may be needed. APPA, LPPC, NARUC, the Canadian Electricity Association, the Edison Electric Institute, the Electricity Consumers Resource Council, the Electric Power Supply Association, the National Rural Electric Cooperative Association and the Transmission Access Policy Study Group all support carefully crafted and specific legislation to deal with the discrete issue of cyber security. We understand the seriousness of the issue, and the need to deal with it. At the same time, we believe that such legislation must be carefully drawn and narrow in its application, to avoid disrupting the mandatory reliability regime that Congress has already required and the electric utility industry is implementing, with oversight by the Federal Energy Regulatory Commission (FERC).

It is extremely important for the Subcommittee to understand that it is in the industry's best interests to protect against cyber security attacks. From the electric utility standpoint, when the lights go out, for whatever reason, we are the ones held responsible. We do not want the lights to go out for any reason, but if and when they do, we want to

be able to bring them back on as quickly as possible, to minimize the potential risks to health, safety, and property, and to minimize the adverse financial impacts on the public. At the same time, our industry is facing additional regulatory requirements in a number of areas, which all translate into increased costs to the consumer. Therefore, it is imperative that we use our dollars and workforce wisely to address the threats and vulnerabilities in the cyber security realm that are most likely to occur, and have the greatest potential impact. This is best accomplished by close collaboration between the government and industry participants rather than "finger pointing" and distrust.

Attached to my testimony is a two-page issue brief that outlines this common perspective among the electric power trade associations, setting out certain shared principles we all support.

Cyber Security Principles

SMUD and the industry coalition believe that legislation regarding the cyber security of the nation's electric power system should be based on certain core principles, and take into account cyber security protection efforts already underway. Any legislation Congress adopts should:

(1) *Continue the strong industry partnership with government agencies in the United States and Canada.* On an ongoing basis, the electric power industry communicates and collaborates in the United States with the Department of Homeland Security (DHS), the Department of Energy (DOE) and FERC. Similarly, in Canada, the industry deals with the various federal and provincial authorities to obtain needed information about potential threats and vulnerabilities related to the bulk power system. The electric power industry also works very closely with NERC to develop mandatory reliability standards, including an array of cyber security standards, which NERC calls "Critical Infrastructure Protection" or "CIP" standards. In addition, NERC, in its capacity as the Electric Sector Information Sharing and Analysis Center (ESISAC), uses its "alert and advisory" procedures to provide participants in the electric power industry with timely and actionable information received from various federal agencies to assure the continued reliability and security of the nation's electric systems. (The ESISAC was established in 1998 in advance of the Y2K issue, and has functioned well since, as noted in NERC's written testimony for today's hearing.) NERC has adopted important improvements to its ESISAC alert communications software that will allow more targeted communications and provide for a more secure, reliable two-way communications pathway between NERC and industry members.

For example, during the Conficker worm outbreak, NERC issued the first alert on October 24, 2008, immediately after Microsoft detected the worm and released its advisory. The alert from NERC included actionable procedures for utilities to implement in order to mitigate the threat of Conficker. As Conficker mutated, NERC issued several updated advisory notices. SMUD and other utilities were

provided with early warning communications containing the information about the threat, which permitted us to implement the control and counter-measures that were appropriate for our utility operations.

(2) *Foster the current electric power industry-wide commitment to continuously monitor the bulk power system and mitigate the effects of transmission grid reliability and security incidents, including cyber security incidents, large and small.* All sectors of the industry are working to instill a culture of compliance with NERC's mandatory electric reliability standards, which are enforced by NERC and FERC within the United States. Maintaining and enhancing the cyber security of our bulk power control and communication systems is a fundamental element of this developing industry culture. The electric utility industry is unlike many other critical infrastructures in the United States, in that each utility company, whether publicly or privately owned, is physically interconnected with and directly affected by the operating practices of its neighboring utilities. This is so because the nation's electric system is interconnected, electricity must be generated and used instantaneously based on the laws of physics, and since electrons follow the path of least resistance as they flow through the system. The very fact that our actions can adversely affect the reliable operation of our neighbors gives the industry a shared responsibility and commitment to reliability and to mandatory and enforceable reliability standards. We are acutely aware that the need to maintain and enhance cyber security presents a new set of potential challenges and opportunities to the industry.

New operational applications made possible by "smart grid" technologies, for example, also may present new vectors for attack upon both new and existing utility systems. On the other hand, manufacturers need to design and utilities need to use smart grid applications that provide new ways of detecting and responding to malicious activity on the electric grid. In addition, the key issue with new "smart grid" devices, either at the bulk transmission level or at the distribution/consumer level, is the manner in which they are developed and manufactured. The electricity industry is involved in the standards development process at the National Institutes of Standards and Technology (NIST) being undertaken to address these new technologies. One key issue is the ways in which these devices communicate. We would suggest that the design should enable communication with a centralized energy management system, similar to the way in which online banking allows communication between an individual and the financial services center, but not among other individuals. This would mean that the energy management system would be the primary place where state of the art cyber security is installed, rather than at the terminus of millions of customers' connections (although some level of security will be needed on the user side as well, again similar to online banking). This is more of a "hub and spoke" approach, and one with which utilities are very familiar. It is also a common risk management strategy – segmenting of networks to minimize risk. Smart grid overlays ought to be segmented to minimize risk exposure to the central "brain."

In response to NERC's Critical Infrastructure Protection Standards, CIP-002 through 009, electric utilities are actively engaged in securing their energy management centers, both physically and electronically. Physical security is being enhanced to institute a six-wall security perimeter, while electronic protection measures include: vulnerability assessments; the securing of access points through firewalls; active monitoring of access points; extensive use of anti-virus and malware protection software; and stronger authentication methodologies. There is also a widespread effort to install complete backup systems in secondary facilities.

(3) *Support continued participation in NERC's industry-based and FERC-approved standards development process, which will yield mandatory cyber security standards for the bulk power system that are clear, technically sound and enforceable, which garner broad support within the industry, and which can be implemented in both the U.S. and Canada on the interconnected North American Transmission Grid.* NERC is striving to draw from the state-of-the-art cyber security controls and countermeasures, through consideration of the NIST framework for cyber security, and to integrate that framework into NERC's existing cyber security standards. NERC, as an organization, and the industry have made a significant commitment of resources to the development of revised and new cyber security standards. In fact, we have committed some of our scarcest resources – our subject matter experts in cyber security and system operations – to the task of developing "second generation" draft standards for consideration by the industry as a whole. NERC has also made important revisions to its standards development process, by putting in place policies that allow, when necessary, for the confidential and expedited or emergency development of reliability standards, including those related to cyber security.

(4) *Be limited to the realm of cyber security.* Some would prefer to include in cyber security legislation "other national security threats" in addition to cyber security threats. SMUD and the industry coalition believe that other government entities, both state and federal, have more direct responsibilities in the general area of national security. Moreover, the electric utility industry has been addressing physical threats since its inception over 100 years ago through existing communication lines between law enforcement agencies at the local and federal levels as well as through its own security measures. SMUD has established strong and long-term partnerships and communications with the Federal Bureau of Investigation (FBI) and Local Law Enforcement Agencies (Sacramento County Sherriff's Department, El Dorado County Sheriff's Department, and Sacramento City Police Department) to aid in response and investigations to Physical Security Incidents or Threats to the Electrical Infrastructures.

SMUD is actively involved and/or part of industry groups that share information and tour facilities to help identify best practices, such as the Edison Electric Institute (EEI) and the

Western Energy Coordinating Council (WECC) Physical Security Working Group (PSWG).

SMUD is actively involved in leadership positions on boards such as the FBI InfraGard Program in which we receive a broad spectrum of information across all of the nation's critical infrastructures as determined by the Department of Homeland Security (DHS). We also have direct contacts with the Regional Terrorism Threat Assessment Center (RTTAC), DHS Office, Office of Homeland Security (OHS – California).

SMUD along with these local law enforcement agencies (LLEA) have conducted numerous Buffer Zone Protection Plans (BZPP) and Security and Vulnerability Risk Assessments of Critical Infrastructures to identify additional measures to better protect these facilities from sabotage or terrorism events.

SMUD's program also consists of effective communications with FERC, NERC and WECC and membership with the Electric Sector Information Sharing and Analysis Center (ESISAC). As a result of our strong partnerships and open lines of communication with these entities, SMUD receives information, key communication and support pertinent to effective protection of our employees, assets and critical infrastructures.

SMUD has established and tested policies, procedures, checklists and training of its personnel to effectively respond and communicate to management and LLEA regarding threats, sabotage, terrorism events and situations as reflected in our preparation for Y2K, 911, and Homeland Security Threat Level Upgrades, etc.

The Subcommittee has also asked me to address electromagnetic phenomena that could affect physical assets. One such phenomenon is a geomagnetic storm. This is solar wind that penetrates the earth's atmosphere and, through the motion of charged ions, induces a direct current on long alternating current lines and can impact the reliability of the grid. Electric utilities that operate in northern latitudes are particularly vulnerable to such geo-magnetic storms. Such phenomena have nothing to do with cyber security, and have existed since the electric grid's inception, as have other types of natural phenomena like catastrophic storms. What we do to address these infrequent types of events is to create redundancies in the system, strengthen key parts of the grid, and establish plans and protocols for restoring electric service. SMUD has established confidential plans and protocols for recovering the electric system in the event of a failure – in fact, we have the ability to reenergize the SMUD system in the event of total collapse of the electric grid. This involves a complex, confidential plan that is comprised of specialized generating units and specific operating procedures that will allow SMUD to begin reenergizing select transmission lines and restoring electric service in a systematic way following a grid catastrophe. WECC and NERC have independently audited our plans and have certified that SMUD meets the requirements to provide this capability.

Another type of electromagnetic pulse can be caused by a nuclear bomb exploding at a high altitude, which cannot be prevented by electric utilities. We depend on the federal

government and military to prevent such an attack. However, NERC has recently established a task force in coordination with DOE to assess realistic measures that can be taken to mitigate risks of outages and equipment damage from this and other high impact, low frequency events.

There are four specific areas in which SMUD and the industry coalition support additional statutory authorities for the federal government and in particular for FERC and DOE:

(1) *Narrowly targeted authority for the FERC to issue emergency orders in response to an imminent threat to the bulk power system.* If the federal government has actionable intelligence about an imminent threat to the bulk power system, and time does not allow for classified industry briefings and timely development of mitigation measures for such a threat, FERC, following consultation with the appropriate governmental authorities in Canada, should be authorized to direct the electric power industry to take needed emergency actions. The electric power industry is ready, willing and able to implement targeted mitigation measures that are clearly linked to the nature of the underlying threat. However, these emergency directives should provide utilities the ability to implement controls related to their operating environment and only remain in effect until the threat subsides or FERC approves related NERC-developed reliability standards that establish permanent measures to address the specific threat. In the United States, Section 215 of the Federal Power Act (added by the Energy Policy Act of 2005) invested FERC with a significant supervisory role in bulk power system reliability. It would be inefficient and confusing to provide potentially duplicative responsibilities to another agency. But at the same time, it would be highly disruptive to the NERC process for development of mandatory and enforceable electric reliability standards set out in FPA Section 215 for the FERC to impose permanent or quasi-permanent cyber security standards that have not undergone the due process steps within the industry required by that section. Further, given that Canadian authorities have already approved NERC's current CIP standards, inconsistent standards in the U.S. and Canada could undermine reliability and potentially make the North American grid more vulnerable to a cyber attack. H.R. 2165 appropriately designates a process for FERC to issue such directives in a cyber emergency.

(2) *Specific authority for the Commission to issue orders that address certain vulnerabilities to the bulk power system identified in the June 21, 2007, ESISAC Advisory issued by NERC, and related remote access issues.* FERC should be authorized to direct that remedial measures be taken by United States entities subject to NERC reliability standards. H.R. 2165 authorizes FERC to carry out such remedial measures. It is important to note that in the two years since the Aurora vulnerability was identified, the industry has taken steps to address the issue, and no cyber attack has occurred similar to the incident the Aurora exercise was intended to simulate.

(3) *Improved communications flows of timely and actionable information from government to industry, matched by enhanced responsibility for the electric power industry to share critical energy infrastructure information with government agencies on a similarly secure and confidential basis.* The industry welcomes secure communication and collaboration with government agencies and the exchange of intelligence information on a particular cyber security threat or vulnerability. It is critical that such information be timely, specific, and actionable as to the nature of the threat or vulnerability to which the utility industry is exposed. After receiving this information, the electric power industry could then direct its expert operators and cyber security staff to take the necessary steps to secure systems and networks, ensuring the reliability and security of the bulk power system. However, it is important to understand that the experts in the utility sector are currently not granted the necessary security clearances to obtain this actionable intelligence information from government and to act as "translators" between the government and the industry with regard to the most effective actions to be taken to secure the grid. We would urge the Subcommittee to consider this issue as the legislation further develops.

While a number of federal agencies have roles in the existing communication process, SMUD and the industry coalition support placing DOE in the role of the lead agency in communicating threat information to the electricity sector because of DOE's decades-long interaction with and understanding of the electric utility industry.

(4) *Enhanced authority for the electric power industry to protect and keep critical energy infrastructure information confidential and non-public.* The electric power industry and government face a variety of complex issues associated with the non-public exchange of Critical Energy Infrastructure Information (CEII) as well as gaining appropriate access to highly sensitive cyber security threat and vulnerability information available to government agencies. For example, NERC and FERC face conflicting statutory obligations to use open, public stakeholder processes to develop cyber security standards and to approve such standards through public notice and comment, while safeguarding from public disclosure threat and vulnerability information that may provide the rationale for certain elements of these reliability standards. Public power utilities like SMUD face their own unique problems in this area. As instrumentalities of state and local governments, public power utilities are subject to state public record and open meeting laws, which make keeping a variety of information non-public more difficult. As publicly-owned entities, this is as it should be – public power utilities are committed to open government and transparency. However, in the case of CEII, transparency is not in the public interest. Just as certain federally-owned utilities may face difficulties protecting information from Freedom of Information Act (FOIA) requests, even when CEII protections are invoked, state and locally-owned utilities face the risk of state record requests for such information. The transfer of such sensitive information to a non-governmental third party makes protection of CEII for public power systems even more

difficult. APPA has developed language to address this issue that we hope will be included as the process moves forward. H.R. 2165 addresses the other areas delineated above.

(5) *Be limited to the bulk power system.* Congress established the Section 215 mandatory reliability structure in recognition that threats to the nation's bulk power system, if actuated, were much more likely than threats to individual distribution systems to create significant effects on national security and our economic interests. This is still true today. Where distribution utilities are interconnected and material in some way to the reliability of the bulk power system, those assets are included in the NERC Compliance Registry.

For a variety of reasons, some policy makers now suggest that physical and cyber assets of distribution utilities must be included in a new iteration of mandatory reliability regulation. They have cited the service of financial and military centers by distribution systems. Some believe that attacks on distribution systems can easily move upstream and impact the bulk power system. Others see the "smart grid" as creating insurmountable numbers of vulnerable system components.

The nature of a load does not alter the fundamental nature of utility operations and the protections built in between distribution components and the bulk power system. Utilities reliably served critical economic and military customers at the time Section 215 was created and implemented. Individual utilities continue to work closely with their critical loads to ensure they are providing the level of service and protection that these customers require. These local, customer-specific relationships provide the foundation for handling threats and vulnerabilities that are targeted against critical customers.

SMUD and the industry hope that Congress will recognize that "critical customers" are not all alike. Many high-tech companies require an extremely high level of service reliability and power quality that cannot be provided from the electric grid alone. On site power conditioning equipment, multiple distribution feeds and even redundant local generation is needed to protect server farms from even momentary interruptions. These customers can and do pay for this superior "five-nines" level of service. Many military bases also require a highly secure power supply, but this supply may or may not require the same level of power quality for the entirety of a particular base's load. A large military base will typically have its own distribution network and may have its own backup generation, complete with an on-base supply of distillate fuel.

Of course, no system – or customer - can be 100 percent secured, but utilities are consistently focused on maintaining a robust level of system protection against any and all threats. Without prompting through legislation, utilities follow a core business practice often called "defense in depth." This means there are protection plans in place in multiple locations between distribution facilities and the bulk power system. For example, utilities use firewalls, intrusion prevention and detection devices and warning systems to deter, prevent and report system

incidents. The utility industry continues to provide its experiences as informed by decades of deploying "defense in depth" strategies when helping to create NERC cyber standards and in implementing them. Utilities are not abandoning their commitment to protect their systems as the smart grid evolves toward integration into the overall utility infrastructure.

Finally, this defense in depth includes recognition that the electric utility industry faces threats to continuity of service on a continuous basis, from small local events such as copper theft from substations and lightning strikes on utility poles, to major regional events such as hurricanes and ice storms. Through our voluntary mutual aid networks, the industry has become quite adept at putting the electric grid back together after such events. After major storms, we share electrical equipment, poles and personnel to get the lights back on as quickly as possible. Federal government assistance is critical during this restoration process, not to lead the effort, but to make sure during major disasters that the electric utility industry and its contractors have timely and preferred access to other infrastructures that are needed to speed restoration.

Additional Comments on H.R. 2165, H.R. 2195, and the Language on Cyber Security Included in Title III, Subtitle A, of S. 1462

SMUD and the industry coalition support H.R. 2165 because it best delineates the necessary new process for the federal government to interact with the industry in the event of a cyber security emergency while not disrupting the existing regulatory structure set forward in Section 215 of the Federal Power Act. In terms of the other legislation that the Subcommittee has asked us to review, SMUD and the industry coalition have some concerns with H.R. 2195 and the cyber security title of S. 1462, including the following:

Inclusion of potentially all electric utility industry assets, including distribution, is overly broad in both H.R. 2195 and S. 1462.
Both define "Critical electric infrastructure" to include distribution systems and assets that if incapacitated or destroyed would have a debilitating impact on national security, national economic security, or national public health or safety. Depending on how FERC and DOE make their respective determinations in implementing the statute, virtually all electric utility infrastructure could be included within the scope of this new statutory authority, even infrastructure in Canada. SMUD and the industry coalition believe that over-inclusion of electric utility infrastructure would be counterproductive; by attempting to protect everything, efforts to protect the truly critical and important infrastructure would be diluted. SMUD and the industry coalition therefore support targeting new FERC and DOE authority toward imminent cyber security threats to the bulk power system in the United States, rather than the broader universe of facilities envisioned in H.R. 2195 and S. 1462. These bills could expose over 1,000 additional distribution systems to FERC and DOE regulation imposing very substantial regulatory and financial burdens on many small cities, towns, and rural areas that are disproportionate to the limited cyber security risks that these facilities and entities pose to the bulk power system, if any. Further, the amount of distribution facilities operated by electric utilities

in the United States vastly exceeds the transmission grid. Platts' 2009 UDI Directory of Electric Power Producers and Distributors reports that there are over 5.8 million miles of distribution lines in the United States (compared to 611,000 miles of transmission lines).

Again, SMUD and the industry coalition believe that the effort to maintain and enhance the cyber security of the nation's critical electric utility infrastructure should focus first on the critical facilities and systems that, if not protected, could contribute to disruption of the nation's power supply.

FERC discretion appears to be broad and unfettered in H.R. 2195 and S. 1462.
Both bills *direct* FERC to issue rules and orders to protect critical electric infrastructure from cyber security threats. This directive imposes no real limits on the extent of FERC authority to order specific actions. As written, it appears that FERC could order the enlargement of facilities, interconnections or disconnections or any other action it deems necessary, without any obligation even to consult with the industry in advance to determine whether its proposed course of action is the most effective and cost-efficient way to address a particular threat. This provision (similar in both bills) would also permit FERC to issue cyber security orders that directly replace or supplement industry- and FERC-approved reliability standards, undermining the carefully crafted reliability regime set out in Section 215. H.R. 2165 allows FERC to take action without obviating the Section 215 and NERC standards development process.

FERC and DOE emergency procedure authorities are potentially redundant in S. 1462.
In S. 1462, FERC and DOE are *both* granted authority to act on an emergency basis without prior notice or hearing for up to 90 days, with FERC authorized to take expedited measures to protect critical electric infrastructure from cyber security vulnerabilities and DOE authorized to take emergency actions to protect critical electric infrastructure from cyber security threats. SMUD and the industry coalition suggest that such emergency or expedited authority be assigned to a single agency, to avoid duplication and confusion as to the respective roles of the two agencies. It is imperative that agency directives not be conflicting.

The requirements to consult with industry and to mitigate burdens before directives become effective should be stronger in both H.R. 2195 and S. 1462.
FERC's authority to issue rules or orders in both bills presumably is subject to the judicial review procedures set out in the FPA, as well the Administrative Procedures Act (although these points should be clarified). DOE and FERC authorities to issue emergency orders in S. 1462 and H.R. 2195 are subject to a 90 day sunset unless FERC "gives interested persons an opportunity to submit written data, views, or arguments . . ." Unfortunately, there is no requirement in either bill for FERC (and DOE, in the case of S. 1462, and DHS in the case of H.R. 2195) to consult with the industry in advance, even as time permits, regarding the nature of the threat or vulnerability, or to take into account the industry's views on the most efficient way in which to address the threat and/or methods for reducing the associated burden on the industry. Moreover, the filing of a request for rehearing or petition for review would not stay the effectiveness of the

directive. Compliance with a potentially flawed directive would therefore be both mandatory and subject to financial penalties under FPA Section 316A (EPAct Sec. 1284).

H.R. 2195 and S. 1462 do not fully address confidentiality issues, including the need for processes governing non-public communications between FERC/DOE and the industry, and the particular confidentiality issues faced by public power utilities. As discussed above, a variety of other communications may need additional safeguards. As noted previously, H.R. 2165 contains provisions that deal with these somewhat complex confidentiality concerns in a more comprehensive and effective manner than do H.R. 2195 and S. 1462, although the latter bills' correctly identify the issue as problematic and could be modified to address industries' concerns. SMUD would also still ask to work with the Subcommittee on some specific concerns relating to state and local sunshine laws that affect public power entities that are not fully addressed in H.R. 2165.

In summary, SMUD and the industry coalition believe the language included in H.R. 2165 properly addresses the necessary, but limited, scope of new federal regulation to address imminent cyber security threats on the bulk power system.

Thank you for the opportunity to present SMUD's and the industry's views on the important cyber security issues facing the electric utility industry. We look forward to continuing to work with the Subcommittee on this important issue and we are available to provide any further assistance.

Mr. MARKEY. Thank you, Mr. DiStasio, very much.

Before I recognize myself, just so everyone understands where we are going here, so we keep these definitions somewhat comprehensible for the audience, we are going to be talking about the bulk power system in the United States. And the Federal Power Act defines that to encompass the large-scale power plants and transmission facilities, but the Bulk Power Act specifically excludes distribution systems. Those are the local systems of lines that bring power from the large transmission facilities, that is, from the bulk power system out to our homes and out to our businesses. And it also specifically excludes the parts of the grid outside the continental United States, Alaska, Hawaii, and Guam. So just so you all understand what we are talking about here as we get into bulk power and distribution systems.

So the Chair will recognize himself; and I would like, Mr. Brown, for you to look at that question of the exclusion of the bulk power system from the distribution systems. Because it is my understanding that there is no clear dividing line dividing the control systems that serve the bulk power system and those that serve the distribution system. So how can we possibly limit the Federal authority to the bulk power system only when it is so interconnected to the distribution system and the fact that that does affect people's homes and businesses?

Mr. BROWN. As State regulators, we are concerned with the whole system from the top to the bottom, including the bulk power system and the distribution system. We have always had this dual jurisdictional aspect to our system whereby the Federal Energy Regulatory Commission oversees the bulk power system, the State regulators oversee the local distribution system. For a hundred years, we have worked together—or since the Federal Power Act, I guess, 70 years we have worked together in maintaining the reliability.

Mr. MARKEY. Here is my question. Since Washington, D.C. is not under the bulk power system, since New York is not, since so much of our military is not, how can you separate them? Shouldn't it be integrated as a single authority here to make sure that there is one system put in place?

Mr. BROWN. The NERC standards apply to all elements of the system from top to bottom. I think when you are talking about cybersecurity, we would welcome Federal leadership in establishing standards for cyber issues, but I think you need to separate——

Mr. MARKEY. The NERC standards only apply to the bulk power system. Would you want them extended over to distribution as well?

Mr. BROWN. I don't think they need to be.

Mr. MARKEY. But aren't they intricately entwined with the local distribution system?

Mr. BROWN. There is certainly the connection between the bulk power system and the distribution system.

Mr. MARKEY. Right. Shouldn't we then integrate it to ensure——

Mr. BROWN. But that doesn't mean that having a centralized authority is necessarily going to be more effective in terms of the reliability of the local system.

I think you need to distinguish between the physical assets, which for a long time have been under the dual control, and the cybersecurity requirements. And, as I say, in cybersecurity requirements I don't think the States would have huge problems with the Federal Government setting standards that apply throughout the system from top to bottom.

Mr. MARKEY. Let me go to you, Mr. McClelland. What do you think?

Mr. MCCLELLAND. Anytime that there is two-way communication between equipment there is a chance to compromise that equipment from a cybersecurity perspective. Deployment of two-way communication devices at the distribution level creates a huge technical challenge to secure that equipment, secure those protocols, and protect the assets up and down the line.

Mr. MARKEY. Ms. Hoffman.

Ms. HOFFMAN. When we are looking at performance measures, if emergency authority was provided as you look at the legislation that was stated as 2195 and 2165, if it is framed as developing performance measures, these performance measures could be implemented either at the State level or at the Federal level. So one could look at the performance measure, and the State utility commissions could consider that as part of their responsibility. So the leadership could be provided at the Federal level under the form of a performance measure.

Mr. MARKEY. Yes. On an ongoing basis, you know, we just have to take note of the fact that when we did have that blackout several years ago, a problem in Ohio affected Canada and New York City.

Mr. UPTON. And Michigan, too.

Mr. MARKEY. I was trying to create the upper point, but you are right, I should have stopped in the continental United States.

By the way, you mentioned Canada in terms of the coordination. Did you include Mexico as well? Are you coordinating with Mexico?

Mr. DISTASIO. Mexico to a lesser extent.

Mr. MARKEY. But Mexico is in?

Mr. DISTASIO. Yes.

Mr. MARKEY. And, Mr. Cook, it is my understanding that over 2 years after the AURORA vulnerability was identified, NERC still has not established standards that would address that vulnerability in an optimal way. Why is that? And how can we possibly argue that the NERC process is adequate, given this delay?

Mr. COOK. The standards are moving in a direction to address some of the vulnerabilities that the AURORA incident disclosed, and we are in a constant process of upgrading those standards. And that is in the process.

Mr. MARKEY. So what is your timeline on completion?

Mr. COOK. The Commission has directed us to give them a timeline for completing the changes to the standards. They recently issued an order, and we are to give them that timeline by the end of this year. We are in the process of developing that timeline right now.

Mr. MARKEY. Are the standards that you are developing specific to AURORA or optimized to deal with AURORA?

Mr. COOK. They don't focus solely on AURORA. They are looking at a range of the threats that the system is dealing with.

Mr. MARKEY. OK. I thank you.

The Chair's time has expired. The gentleman from Michigan is recognized for 5 minutes.

Mr. UPTON. Thank you, Mr. Chairman.

Mr. McClelland, Mr. Brown said in his testimony that the CIP standards already in place are adequate for both physical and cybersecurity. Do you think that is accurate?

Mr. MCCLELLAND. No, the Commission directed an order 706. When we approved the eight standards, we directed modifications to every standard. Some are very substantive and significant. I mean, I could provide specific examples as to why they are not adequate, but they are not adequate yet. There are still significant gaps.

There is also a significant lag as far as compliance with the standards. Only the most experienced and largest entities that fall under bulk power system jurisdiction have to be compliant with the standards today, and only 12 requirements of the standards do they have to be complaint with. It is a phased-in implementation.

Mr. UPTON. Ms. Hoffman, would you agree with that?

Ms. HOFFMAN. Yes.

Mr. UPTON. Mr. McClelland, can you describe for us, the members here, as well as the audience, what an EMP attack would be? What are the dynamics of that?

Mr. MCCLELLAND. There are two sources of electromagnetic pulse. One source is naturally occurring. It is a solar magnetic activity that disturbs the Earth's atmosphere, magnetic fields, and ionosphere. It rolls them back, if you will. During that rollback time, the Earth's magnetic fields are disturbed. It collapses back on itself; and that produces ground currents, geomagnetically induced currents. Those currents travel through the earth; and everything that they hit on the bulk power system they wreak havoc on, particularly large bulk power system transformers. They will destroy those transformers within a matter of seconds if they haven't been mitigated against such an occurrence.

There is also——

Mr. UPTON. No, go ahead.

Mr. MCCLELLAND. There is also manmade EMP, electromagnetic pulse attacks. Those generate three separate times of energy disbursement. One is termed an E1. It happens within a billionth of a second. It is a very high, very strong radio frequency type energy burst. The wires and the transmission wires and facilities act as antenna. They pick that burst up, and it destroys all control equipment.

Very shortly thereafter, there is an E2 effect, which is similar to lightning. Utilities are very well mitigated against lightning. However, after an E1 burst, it is really uncertain as to how much more devastation it would cause.

And then, finally, there is the E3 effect, which is the first effect I described that happens naturally, every so often.

Mr. UPTON. And how difficult is it to build a manmade device that would emit these EMPs?

Mr. MCCLELLAND. It is not difficult. For a nation state, for a sponsored terrorist organization, it is not difficult. And it is getting easier all the time.

Mr. UPTON. And can you tell us about what the cost might be?

Mr. MCCLELLAND. I don't have any information about cost. For a small—if it is a radio frequency weapon, a small RFI platform, those are less than a hundred thousand dollars apiece. Those can be portable, and they can be directed—you have to be pretty close to your target, but if you are close——

Mr. UPTON. Pretty close, within a quarter mile, a hundred yards?

Mr. MCCLELLAND. Within hundreds or thousands of feet, depending upon the quality of the weapon itself. It is certainly possible to put a small portable weapon in a vehicle-mounted platform and direct that at facilities.

Mr. UPTON. And our bulk power distribution system, it would be pretty vulnerable to that type of attack, is that right?

Mr. MCCLELLAND. The Commission doesn't have any information as far as what folks have done or haven't done regarding EMP mitigation. We suspect there hasn't been a lot of activity there.

Mr. UPTON. And, again, that is a physical attack, not a cyber attack.

Mr. MCCLELLAND. That is correct.

Mr. UPTON. And, Mr. Brown, as you indicated, you believe that H.R. 2165 is the best approach. H.R. 2165 looks at only cybersecurity. As I understand it, it does very little for physical security. So if what your statement is on page 5, that CIP standards already in place are adequate for both physical and cybersecurity, how does that comport to an E1 or, obviously, E2 or E3 as it relates to the distribution of that power across not only New York but all 50 States?

And that is sort of the crux, as we look at the two different bills before us, H.R. 2165, which you said is the better bill, does not have physical security. It does not include Alaska, Hawaii, Guam, New York, or as it gets to, as the chairman said, the distribution.

I just don't know if you have had access to classified reports, as some of us were able to participate last week. Mr. McClelland was part of that discussion that we had. But I just want to know what evidence you have as you indicate that the present standards are adequate.

Mr. BROWN. Well, obviously, I don't have access. And that is one of the concerns that we have, is we don't necessarily have access to some of the newer threats that are emerging. All we can judge on is what we know and see.

There are a variety of threats to the electric system besides EMP. You can take out an electric system in a variety of different ways, and that is why we have been trying to work with NERC on the broad array of security requirements that are necessary to protect the system. And that is why I pointed out the difference between a threat and a vulnerability.

If there is an active threat out there, I think everybody needs to know it; and I don't think any of the legislation at this point kind of has a mechanism in place that if there is a threat that there is a way of sharing that threat with all of the State jurisdictional agencies, law enforcement agencies that are going to need to ad-

dress that threat. I am not sure a single standard somewhere established in legislation is going to be able to solve that problem or a new threat won't arise.

Mr. UPTON. Our time has expired.

I just ask one quick question of Mr. McClelland; and that is, as they see threats that come in, it is too late if they are imminent. We have to be prepared. And I would presume that is why we need legislation very quick. Correct?

Mr. MCCLELLAND. Right. Right. That is correct.

Mr. UPTON. I know my time has expired.

Mr. MARKEY. The gentleman's time has expired.

The Chair recognizes the gentleman from California, Mr. McNerney.

Mr. MCNERNEY. Thank you, Mr. Chairman.

Mr. McClelland, I want to thank you for hosting me when I visited FERC and alerting me to the AURORA vulnerability at that time.

You discussed in your written testimony the challenges posed by smart grid technology. In your opinion, are the local utilities aware of this vulnerability? And, if not, what can we do to enhance that lack of preparation?

Mr. MCCLELLAND. We have an expression inside the Commission that the utilities are out in the wild. What that means is that they haven't really been brought in and briefed about the level, the sophisticated level of threat that could occur with cyber vulnerabilities, with two-way communications. I think that is evidenced by some of the activity that happens at other Federal agencies, Department of Defense, and sophistication of the levels of defense that they employ versus a utility that may be not as sophisticated in that regard.

Mr. MCNERNEY. Thank you.

Mr. DiStasio——

Mr. MARKEY. Mr. DiStasio, he is not talking about a utility in Silicon Valley. So you shouldn't take that personally, but——

Mr. MCNERNEY. You mentioned that utility sector experts are not necessarily cybersecurity experts and lack high-level security clearances. Is there a particular path forward to remedying that problem that you envision?

Mr. DISTASIO. Well, because of the emerging technologies, I will say this has really evolved over time as the electric grid has become operated in a more digital way, more SCADA controls and so forth. There has been a greater integration of the physical operators of the system and the technologists, and we actually both participate through the NERC process but within our own utilities. And we use what is called a layered defense in depth process where we look at people and technology and operations, controls that address both physical and cyber segregation of our systems, protection of our systems, control of information, training, and access to the individuals. So that is actually under way in most utilities across the Nation. I will say the diversity of our systems leads us not to be able to necessarily have a one-size-fits-all way to resolve that issue.

Mr. MCNERNEY. Thank you.

You know, it seems to me that the real question here is how much additional authority is needed to approach this problem.

Thank you, Mr. Brown, for bringing up the distinction between immediate and imminent threat versus vulnerabilities. When you look at 2165 versus 2195, 2165 is a little bit more specific and a little bit more limited range, whereas 95 is not as specific but has a broad range. I would ask anyone now on the panel, is there a utility preference for those approaches? For which one of those approaches would be preferable?

Mr. DISTASIO. I would like to respond to that.

From the industry perspective, 2165, as I said in my testimony, would be preferential, because I think it is very important to distinguish between vulnerabilities which need to be dealt with on a continuous improvement basis over time on a proactive and a preventative measure versus immediate and imminent threats or emergency issues that we need confidential information to be able to respond to quickly. And so we think that 2165 best addresses that differentiation.

Mr. MCNERNEY. Any other responders on the panel to that question?

Mr. BROWN. Just that, in 2005, the authorization for NERC, I think a lot of progress has been made along the way in trying to address the vulnerability question, trying to set standards for the vulnerability question.

I think what makes the threat issue is where we believe the focus might be best served for this legislation, is that there be more—an ability, a process established by Congress that will say, if there is an imminent threat, exactly what the process will be in terms of disseminating that information to State regulators, utilities on a confidential basis so that we can all address this together. I think that is the most important part of the legislation. That kind of reinventing what has already been done in 2005 and trying to move it again may be a step backward instead of a step forward.

Mr. MCNERNEY. My final question, if I have a little bit of time, Mr. Cook, I was involved in setting standards in my prior life; and it is kind of an interesting process to get people to agree on these things. So how is that working out? I mean, are your participants finding ways to agree on these things and then the broader utility network buying into those agreements? Is that what is happening?

Mr. COOK. As a general matter, that is right.

Mr. MARKEY. The gentleman's time has expired. The witness will please try to answer the question.

Mr. COOK. Thank you.

The industry has stepped up and is providing experts and is working through the process. As I mentioned earlier, it is a continuous process of improving these standards, and we are making that progress.

Mr. MARKEY. Thank you.

The gentleman's time has expired.

The Chair recognizes the gentleman from Texas, the ranking member of the full committee, Mr. Barton.

Mr. BARTON. Thank you, Mr. Chairman.

I am sitting here thinking what a perk it is to have you chairing a hearing with FERC and NERC, while the terrorists are smirking

and lurking around. It is somewhat of a Herculean effort on your part. We appreciate it.

Mr. MARKEY. Excellent. I will try to respond before the end of your comments.

Mr. BARTON. You are going to have to work to beat that. Of course, I had 10 or 15 minutes to think about it.

Mr. MARKEY. I think we should give the gentleman his full 5 minutes and note the incredible——

Mr. BARTON. I am going to work on SMUD, too. We will see if we can get something done that is not vulgar on that.

Anyway, I would ask Mr. McClelland and Mr. Cook—or Dr. Cook—to comment on the relationship between the bulk power system and the distribution system and if you feel that the Federal Government should preempt the States in looking at this issue with regard to the distribution system.

Mr. MCCLELLAND. I can start.

The bulk power system is generally defined as 100,000 volts or above. The legislation EPAC 2005 required the Commission to approve standards—review and approved standards for the bulk power system. However, it is defined by the regions. And so a region that chooses to redefine the bulk power system as, say, 200,000 volts and above can exempt 60 or 70 percent of the transmission facilities within that region by redefining the term "bulk power system." So I think it is important to make the distinction that it is not just distribution that would be excluded under bulk power system. It may also be what is traditionally considered transmission facilities that serve major metropolitan areas that could be excluded by that definition.

Now, back to the term "distribution facilities." It does—the legislation does exclude facilities used for the distribution of local energy, which would be the facilities that would capture, say, the meters on the homes, smart meters, and any cyber facilities where appliances within the homes that communicate to the meters that may communicate then back to the transmission systems. And from an oversight perspective, from a reliability standards perspective, it is extremely difficult to regulate that communication without that ability, without that jurisdiction.

Mr. BARTON. Mr. Cook.

Mr. COOK. For us, it is a matter of priorities, that the consequences are most profound at the bulk system level. And that is where our focus has been, and that is where we believe the focus needs to be.

Mr. BARTON. Would the witness from the Department of Energy want to comment on that?

Ms. HOFFMAN. Any leadership that FERC provides in developing performance measures to protect the reliability of the bulk power system could be applicable to the distribution system if the State PUC regulators decide to choose and follow them.

Mr. BARTON. Mr. Chairman, I am going to yield back. I think, to be really serious, this is a very serious hearing, and I am glad you are doing it. I would hope, though, that we could legislate at the Federal level without impinging too much on the local or the State level for distribution systems. I would be reluctant to be too bold in preempting the States. But I think this is an important

issue, and I am very glad that you and Chairman Markey are addressing it in the way that you are addressing it.

And with that I yield back.

Mr. MARKEY. Thank you, Mr. Barton, as well. I thank you. You have drawn our attention to this issue in another way that, for better or worse, there is a quirk that NERC and FERC do not have——

Mr. BARTON. I almost used quirk.

Mr. MARKEY [continuing]. Do not have that jurisdiction; and, as a result, some jerk could hurt the system. And we have to close that regulatory black hole here.

Mr. BARTON. Great minds think alike, Mr. Chairman.

Mr. MARKEY. I am not sure other people are viewing us that way. But I thank the gentleman.

The Chair recognizes the gentlelady from Wisconsin.

Ms. BALDWIN. Thank you, Mr. Chairman.

One very specific question and hopefully followed by a broad, open question.

In our briefing memo from committee staff, we have our attention pointed to physical vulnerabilities of the grid. And I am just going to read you an excerpt.

For example, large transformers, essential to the reliable operation of the grid, are manufactured outside of the United States; and replacement may require up to 2 years. A limited number of spare large transformers are available within the United States; and industry has developed a program, the Spare Transformer Equipment Program, or STEP, another acronym, providing for sharing of such assets in the event of a terrorist attack. Any policy recommendations of how we can—and I will ask you, Ms. Hoffman, recommendations for how we could be more prepared in the event of an emergency?

Ms. HOFFMAN. You bring up a very, very important point, that critical to the reliability of the bulk power system is the recovery of that system. So an important aspect of that is the focus on manufacturing and manufacturing capabilities in the United States. So as we look at developing protection mechanisms, we must recognize that some parts of the grid will go down. So another key aspect is how fast can we restore? And that is directly to your point, which is very important.

Ms. BALDWIN. What is our domestic manufacturing capacity and what are we doing to bolster it?

Ms. HOFFMAN. For large transformers, very limited. In fact, I think there is only one company that will be looking at large transformers.

Ms. BALDWIN. Thank you.

On a much broader question for all of you is the issue of communication and information exchange. And we have had testimony from the State perspective, from the NERC perspective of the frustration being that much of this is classified and tightly held and needs to be communicated to actors with the ability to prepare and plan; and yet we have sensitivities with getting certain information out. We have been grappling with this as a committee on previous legislation relating to chemical plant security, with water treatment plant security, now in this arena.

I know it is a very broad question, but I would like to hear your perspectives on how we get the information that we are learning at the Department of Energy and FERC to the hands of the people who actually need to plan and help us prepare, while protecting that information carefully. And we haven't even talked about ISOs, but they are another level of all of this.

And if you wouldn't mind, just starting with Mr. McClelland and going through the panel, that would be helpful.

Mr. MCCLELLAND. One of the problems we had with the AURORA advisory, the advisory went out by NERC in June, and the Commission was asked to do follow-ups to determine how effective the mitigations were put into place. We couldn't protect the information, or felt that we may not be able to protect it from a FOIA request, and so we ended up asking for industry volunteers and reviewed their plans one at a time without taking any information back to the Commission. This information transfer, the inability to protect the information, severely impeded folks' ability, the entities' ability to implement mitigation strategies.

Now, we saw a whole gamut. I don't want to say that was the only reason. There were some folks that were very well mitigated. There was good old-fashioned American ingenuity that had been deployed, but there were other entities that did nothing, and additional information didn't appear as if it would have helped. So we have asked that any additional authority that be conveyed provide the ability for the Commission to protect that information.

Ms. BALDWIN. Briefly, Ms. Hoffman.

Ms. HOFFMAN. Briefly, point one, clearances. I think there has to be a wider, greater distribution of appropriate levels of clearances across the electric sector. Two, we need to protect the information from FOIA requests in accordance to—very similar to maybe what DHS does with their Critical Information Act.

Ms. BALDWIN. Mr. Brown? Any comment on the communications issue?

Mr. BROWN. We deal with confidential information at the State level all the time in terms of information regarding the bulk power system. I think we are well prepared and positioned, if we get the information, to protect it and use it.

The electric systems run on contingencies all the time. That is how the electric system is run. It is always planning for the worst thing that could happen; and that, if it happens, the system will stay up because there is adequate backup. Obviously, the more information available about threats, the better that contingency system can work.

Ms. BALDWIN. Mr. Cook.

Mr. COOK. We have been successful in the last year in arranging for cleared briefings for some CEOs to have access to some more of that information. More of that needs to happen.

I agree with Ms. Hoffman that the clearances program needs to be accelerated, and there needs to be a way that this information can get out to folks without them having to make it public. The State Open Records Acts sometimes get in the way of that, because anything that some State agencies get has to be made public then.

Ms. BALDWIN. Mr. DiStasio.

Mr. DISTASIO. I would agree with Mr. Cook. I think that is an important step for Congress to consider. Because, right now, without adequate clearance, the information we might get would be limited and not applicable to a pending emergency or vulnerability that we are the ones responsible for addressing. So we certainly support additional clearance levels to make sure that threats can be dealt with in a timely manner and confidentially.

Mr. MARKEY. The gentlelady's time has expired.

The Chair recognizes the gentleman from Illinois.

Mr. SHIMKUS. Thank you, Mr. Chairman.

If you all would just, if you have got a piece of paper, scribble down solar storm, radio frequency, EMP, and then cyber. And then my first question—there is two questions—I would ask you to prioritize the threat as you see it in those four categories, and then I would ask you to prioritize costs of recovery.

And kind of following up on my opening statement about where our focus should be, I think sometimes we don't really know what is the biggest threat, what is the biggest cost recovery.

And so if I could start with Mr. McClelland and just go down the line, if you all could do that for me. And if you don't want to, you don't have to, but I mean, if you could, that would be helpful.

Mr. MCCLELLAND. That is a difficult question.

Mr. MARKEY. Who wants to be a millionaire? If you can rank them one, two, three, four, and then we can fill it in.

Mr. MCCLELLAND. Tough to do. Cyber I had as one; solar storms I have as two. And, in fact, solar storms could be one because they are inevitable. We are going to get another storm. We are going to get another 1921 event, which has been called a one-in-100-year storm. That is going to happen. And, if it does, it will be devastating consequences.

RF weapons and EMP would be the next two on the list.

Mr. SHIMKUS. Was radio frequency third or EMP third?

Mr. MCCLELLAND. I put RF weapons third only because they are so affordable and easier to tote, and EMP weapons fourth.

Mr. SHIMKUS. Thank you. And I will come back to the costs.

Ms. HOFFMAN. I did cyber as one, RF as two, solar storms as three, and EMP as four.

Mr. SHIMKUS. Great.

Mr. BROWN. I want to emphasize cyber as one. These people are much more of experts and able to judge the vulnerabilities. But we are about to introduce—perhaps the President has already announced—billions of dollars of new moneys to allow——

Mr. SHIMKUS. Let me stop you there, because I do have that. It is a Washington Post article today. President Obama plans to unveil Tuesday $3.4 billion in grants to smart meters, updated transformers, and other devices. Is that where you are headed?

Mr. BROWN. Yes, exactly. And the point is there is going to be a whole new system of two-way communications introduced to the electricity industry that really——

Mr. SHIMKUS. Does that make that more secure or less secure?

Mr. BROWN. It can be both. It should be more secure. More real-time information about the system should be good. But it introduces new vulnerabilities to the system, which if not protected is bad.

Mr. SHIMKUS. All right. I have limited time. So you talked about cyber, so cyber—what is your priority?

Mr. BROWN. Cybersecurity would be, far and away, number one. I was going to say two, three, and four I am not really that capable of assessing.

Mr. SHIMKUS. OK. Great.

Mr. Cook.

Mr. COOK. I would put cyber at a very high number one, solar after that. And as between RF and EMP, I am not sure.

Mr. SHIMKUS. Great.

Sir.

Mr. DISTASIO. I would also put cyber number one. And, frankly, I would like to consult with the industry. Because I put two, three, and four again——

Mr. SHIMKUS. OK. Let me go back to cost of recovery, if any of you could do that based upon these attacks.

Mr. MCCLELLAND. EMP and RF weapons I would put as number one. And I would rate them the same because it is the same mitigation for either of those two. Cyber I would put as number two. That is highly dependent, though, on what the utility has or has not done. And solar I would put as number three as far as the least-cost alternative.

And I do want to add that in the original grouping I don't have these—although I ranked them for you, I don't have them very far apart.

Mr. SHIMKUS. Yes, thank you. And I am going to stop there because I am on limited time.

I want to highlight that on April 21st, 2009, a study by the National Academy of Scientists found the U.S. could suffer one to two trillion in damages as a result of EMP; and it would take four to 10 years to fully recover. By contrast, Hurricane Katrina inflicted $150 billion to $300 billion in damage. So this is my fear or concern.

I have a wind generating power plant that went down because of an Internet connection, and it went down for 10 or 15 days. Bespeaks to the greening of America and the reliability of electricity.

The other issue that I wanted to address, although we have kind of covered it, this also speaks of my opinion, everybody knows I am a supply guy here on this committee, more generation versus less. If we limit the ability for us to increase generation in America, we increase the ability to put ourselves at risk when any one, two, or three of these are targeted. So I would be in support of a position that says let's build more power plants, not less.

And thank you, Mr. Chairman, and I will yield my remaining time. Thank you, Mr. Chairman.

Mr. MARKEY. The gentleman's time has expired.

The Chair recognizes the gentleman from Georgia, the sponsor of the bill, Mr. Barrow.

Mr. BARROW. I thank the Chair.

The table has pretty much been set for the issues that we are going to be taking under deliberation in negotiations going forward on this. But one thing that hasn't been talked very much about, and it is an issue that is very much on the minds of the folks who are going to be tasked with following or implementing any policies

that we are going to be authorizing the implementation of, and that is with the electrical industry, the generators and the distributors.

So I want to talk just briefly, at least kind of set the stage for those discussions by asking if any of you all can identify any issues of disparate treatment or disparate impact that might result from the kinds of rules that we are all talking about trying to create and authorize here? Can you foresee, looking down the road, that there might be any disparate impacts in terms of some of the mandates that might be forthcoming? Impacts that might be disparate in terms of whether or not you are a big guy, a big for-profit utility company as opposed to a little guy, an EMC, whether any regional impacts that you can see as a result of the mandates that we are contemplating here.

We all want to do the right thing, and I know the generators and distributors all want do the right thing. But I am sure that as there are staggering costs we are trying to avoid, there are going to be some costs we are going to incur along the way.

So the first thing I want to ask is, can anybody here on the panel give us some idea as to the kinds of costs and especially issues of equity and fairness, disparate impacts that might result from any of the mandates we are talking about today?

Mr. Brown, I think you are sort of on the hot seat representing the utility commissioners of the country. Why don't you go first?

Mr. BROWN. Sure.

I am not sure about disparate impacts, but I think you need to put this into a context. If there is a federally mandated cost that we have got to recover from our rate payers, it means perhaps we won't be able to do something else that we have been trying to do.

Mr. BARROW. An opportunity cost, in other words.

Mr. BROWN. Right now, at the State level, we are collecting money for renewable portfolio standards. Over 30 States have that. Energy efficiency programs, infrastructure needs, new transmission. So there is a lot of pressures already on electricity rates.

Mr. BARROW. What kind of costs do you foresee? What kind of magnitude?

Mr. BROWN. Billions of dollars on a State level, tens of billions of dollars on a national level. At the same time, customers that are over 60 days in arrears on their bills—in New York over $600 million is in arrears. That is up 25 percent from a year ago. So just the rates that we have today, people are unable to be able to pay it.

So I guess my concern is the more mandates that we get requiring expenditures is going to mean dollars that we are not going to be able to collect to do other things that we really want to do maintaining the reliability, safety, and efficiency of the system.

Mr. BARROW. Mr. McClelland, Ms. Hoffman, do you all have any thoughts to suggest along these lines? What do you foresee?

Mr. MCCLELLAND. As far as disparate treatment, the generators that don't fall under tariffs before the Commission, any generators that have, say, cost-based contracts or contractual arrangements would not necessarily qualify for security upgrades for cybersecurity or for, say, EMP expenditures. So that would have to be addressed.

There may be—and I won't speak to the particulars, but there may be utilities or entities under cost freezes. They may be under rate freezes within different States. And that treatment or security upgrade would have to be considered by the State commissions, especially if it was a security upgrade necessary for distribution systems, say, smart metering upgrades.

And as far as whether or not we incur the costs, I think the threat is here. The vulnerability is here, and the threat is here. This is a different world. There are entities that are intent—they believe that the bulk power system in the United States, the electric grid, is a legitimate military target; and they have set their sights on that system. And so whether or not—the costs are just going to have to be incurred. We are going to have to address the issue.

Mr. BARROW. Any way you slice it, the costs of prevention are a whole lot smaller than the costs of inaction is what you are saying.

How about you, Mr. DiStasio.

Mr. DISTASIO. I would just want to add, from the industry perspective, the actual NERC regime that was enacted in 2005, we have already added significant compliance resources and industry experts to that at a cost of a fair amount of money. And one of the reasons that we are actually supportive of the approach that you are taking to this is it does tend to appropriately focus this on emergency threats, which to me that represents a much smaller cost.

I think I mentioned the fact that we have 400 miles of transmission but 10,000 of distribution, which is not uncommon for many utility systems; and if you look at the expansion of taking it down to lower probability assets in the distribution system, it adds significant costs without certainty that that is going to have the same disruptive effect as the bulk power system.

Mr. BARROW. Thank you.

My time has expired. I would like Ms. Hoffman to feel welcome to respond, but my time has expired. Thank you, Mr. Chairman.

Mr. MARKEY. The gentleman's time has expired, but real quick.

Ms. HOFFMAN. Real quick the only comment I would add is one size reliability does not fit all. Defense Department, manufacturing industries require higher level of reliability than, say, residential customers or what they are more willing to accept. On-site generation, micro grids, UPS systems are alternatives to look at as we consider reliability.

Mr. MARKEY. Great. Are there others who wanted to say a word? No.

The gentleman's time has expired.

Mr. McClelland, do you want to say a word here?

Mr. MCCLELLAND. I had an opportunity.

Mr. MARKEY. OK. Good. Great.

The Chair recognizes the gentleman from Texas, Mr. Burgess.

Dr. BURGESS. Thank you, Mr. Chairman.

And, Chairman Brown, I was particularly intrigued by your comments, how much are we willing to pay for marginal increases in security? And obviously that is the fine balance that we have here today. And I don't know if I have a—conceptually, if I have a good idea of the number of dollars that it would take to harden our grid

against an electromagnetic pulse, either whether it is generated by natural occurrences, by a solar flare, or a legitimate military target, as was outlined by Mr. McClelland.

Can you give us some sense of the task ahead? If we were to have a grid that was completely impervious to anything versus what is actually practical, what are the cost differentials that we are talking about?

Mr. BROWN. We have infrastructure needs at State regulatory levels of billions of dollars just to maintain the existing aging system. The idea that you could make it impervious I think is tens of billions of dollars of investment. It is an entirely new and different way of doing the system.

Earlier, we talked about the bulk power——

Dr. BURGESS. Can I stop you there?

Do we, in fact—does the technology exist to do that if dollars were not an issue? Do we have the technical know-how to do that?

Mr. BROWN. It is a matter of duplication. You can duplicate a lot of the system over and over and over again so that technically—I will leave it to some of the experts whether it is completely impervious, but that is a lot of money.

And this is all a cost-benefit analysis. I think that is what regulators do all the time, is cost-benefit analysis. I could gold-plate the electric system in New York and make sure that we don't have as many outages, but the costs might be two to three times—the rate payers, they would find it unaffordable to pay the rates that are out there.

It is always a balance between reliability and cost, and you can't just look at cost because you would have an unreliable system. But you can't just look at liability, because you will have a gold-plated, expensive system. Tough balance.

Dr. BURGESS. On balance, the legislation that is the subject of this hearing, do you think we are threading that needle appropriately with trying to balance those two ends?

Mr. BROWN. One of the concerns I had about some of the legislation was it is reaching down all the way into the distribution system, which was the chairman's first question.

And I will note that, for example, the three major blackouts we have had in New York City, ranging from 1965 on, were all bulk power system disruptions, problems that the bulk power level got to the local level. It wasn't problems with the local system.

So spending a lot of money on the local system and then perhaps sacrificing some things being done on the bulk power system may not be a cost-effective way of meeting the concern. That is why we would like to see the focus on the bulk power system, and we think the work that began in 2005 with NERC is the appropriate way to be moving towards that goal.

Dr. BURGESS. And yet I mean there are technologies available today that weren't available 5 or 10 years ago. And those technologies do, as I think you pointed out in your testimony, add increased vulnerabilities in different ways.

With this legislation, are we taking an appropriate over-the-horizon look at what may be available to electricity consumers in the future in providing them the protections? Or are we looking at a situation where we may have to be back here in 5 or 10 years, 15

years and revisiting this entire issue? Do we have the appropriate eye on what is coming down the pike for the future?

Ms. HOFFMAN. In order to prevent that, I think we need to do a continual risk evaluation of what the new threats are and the new concerns are, as well as what the new technology is so that we can keep feeding and cycling through that loop so we stay ahead of the game.

Mr. BROWN. And that is why I also emphasize cybersecurity. That is the new element that is coming into the system. The smart grid two-way communications, we really need to get that secure. I think that is the most important focus at this point in time.

Dr. BURGESS. I was just back home. There was an effort to go to smart meters, and then they turned out to not be in compliance with what we said they ought to have. And so you have got a company down there now that is asking its rate payers to pick up the millions of dollars for meters that aren't going to be able to be used. We do have to be careful how we implement these things, because we can end up costing people a lot of money for very little return.

And at the same time, as Mr. Shimkus points out, the far end of the scale is we may be asking for hundreds of billions of dollars of investment to protect us against trillions of dollars in loss and decades of recovery.

So thank you, Mr. Chairman. I will yield back.

Mr. MARKEY. Great. The gentleman's time has expired.

The Chair recognizes the gentleman from Utah, Mr. Matheson.

Mr. MATHESON. Thank you, Mr. Chairman.

I have heard some different opinions about whether or not utilities receive specific actionable intelligence from the Federal Government regarding imminent cyber threats. And so I was wondering—I would ask all the witnesses or anyone to respond—what your thoughts are about this and do you think utilities should receive more clearances or more information?

Mr. DISTASIO. I could address that from the industry perspective. To date, we have not received any notifications or specific actionable intelligence relative to imminent threats. We did have the information that has been discussed regarding AURORA. There were 30 utilities, as was mentioned, that worked on a voluntary basis to try to understand and mitigate that.

I do believe we do need additional clearance. Because while there are many reports out there that there are significant threats and while there have been briefings that suggest that these things are real and imminent, the utility industry to date has not been notified with any specificity in order to best mitigate those or prevent them. We do work through the NERC standards on a prospective basis, but we do think that additional confidential clearance and additional ability to get additional Federal authority to provide specific and actionable information would be very helpful.

Mr. MATHESON. OK. Thanks. Yes.

Mr. MCCLELLAND. I guess I want to be very clear right up front, the NERC standards are wholly inadequate to address threats to national security through the power grid. The NERC standards, on average, take 4 years to develop. Modifications, many different iterations. They are done in an open and inclusive forum. So not

only is the reason for the standard published but also all the proposed mitigation strategies, and bad guys have access to the Web sites and can look at those proposed mitigations.

So the NERC standard—the existing standards that are in place, the Commission has identified substantial security gaps in those standards, directed modifications, and are awaiting the NERC process to finish the modifications.

As far as information to utilities, yes, I agree utilities do need more specific information to be conveyed. But it is not just the information. In the AURORA advisory which was issued in June, there were very specific mitigations that were requested. An advisory is voluntary. There is no ability for any Federal agency to direct utilities to take action to protect their systems in the event of a threat or a vulnerability. So the advisory was voluntary, and we saw compliance that wasn't great. We didn't see great compliance even with entities that understood the issue. However, everyone could have benefited by additional information.

Mr. COOK. Just to answer your question, the feedback we are getting is that more specific actionable intelligence information is what is needed. That is the feedback we got on AURORA. There were limits on what could be said. So it is a combination of clearances to the industry and figuring out ways of having—arranging a classification of information such that it can get out. Both of those are important.

Mr. MATHESON. OK. I appreciate that.

Mr. McClelland, I was going to ask you if the new Federal authority that issues cyber emergency orders is too broad. That could also cause some other unintended consequences. Do you have thoughts about where we get the sweet spot on this?

Mr. MCCLELLAND. Yes, that is very difficult. The authority has been called extraordinary. It is extraordinary authority. And the Commission is not an intelligence agency. Some may say we don't even have intelligence. But we don't collect intelligence. So we would depend on other agencies such as DOE, DHS, DOD, CIA to bring vulnerabilities and threats that would endanger national security, use our authority then to order mitigation. It is very specific mitigations that may be targeted at very specific utilities for a limited period of time. That is much more targeted and specific than, say, a standards action might be.

Mr. MATHESON. OK. And can I ask you, do you have thoughts about steps the Federal Government could take to—you heard questions about costs from other members. Do you have thoughts about how the Federal Government could work with utilities to help mitigate the cost impact relative to the risks that we are trying to address?

Mr. MCCLELLAND. Yes. We had the benefit of reviewing with the utilities. We asked for 30 volunteers and did get 30 volunteers on the AURORA mitigation. We had the benefit of spending a day with each of those utilities, and there were some very good ideas that came from the utilities back to the Commission. So it would be an iterative process.

The Commission would have to move quickly. If it was a vulnerability or threat that endangered national security, we would issue that. There would be a hearing process or a back-and-forth process

where alternative practices could be proposed by the utilities to accomplish the same purpose but nevertheless not delay the mitigation being put into place to protect the economy, its citizens, and the military of the United States.

Mr. MATHESON. Thank you. I yield back, Mr. Chairman.

Mr. MARKEY. The gentleman's time has expired.

The Chair recognizes the gentleman from Oregon, Mr. Walden.

Mr. WALDEN. Thank you, Mr. Chairman.

So I want to see if I have this right. Basically, folks in the power industry don't get the information of the specificity of the threat that they are supposed to figure out how to deal with. Right? I mean, isn't that what you are saying?

Mr. DISTASIO. What I said was, to date, there has not been any specific actionable information provided. Not to say there aren't vulnerabilities, but there has not been an individual threat that has been communicated beyond this AURORA test.

Mr. WALDEN. And yet we know there are, Mr. McClelland, to the extent you are able to talk about this, that there are fairly specific threats. Well, we all know every computer it seems like is being attacked by somebody at some point. And so how do we bridge this? It would seem to me with so much on the line that there must be a way that we can communicate the information you need to understand how serious this is and to cope with it. I understand you understand how serious it is. How do we bridge that?

Mr. DISTASIO. I want to be very clear on one point. The utility industry has been dealing with vulnerabilities maybe that originated from reliability and now much more security and cyber-based for many, many years and will continue to do that. So we are not awaiting information to do that. However, if there is a gap, it is around this issue that there is a lot of discussion around pending threats that seem to be more imminent that have not been communicated; and we just need to understand what those are so we can best mitigate them on the ground within our systems for the consumers.

Mr. WALDEN. And is the issue here that you want to know the very timely, specific threat, as in X organization is going to do Y to your system, or is it—is there anything you are not doing now to protect your system that that kind of information would help you protect?

It would seem to me it is pretty clear where the threat—not where it comes from from a specific individual or organization necessarily, but there are only so many ways to get into your system and do damage. And I guess that is the question. You would think you would know what those ways are and be set up to mitigate, right?

Mr. DISTASIO. And we do believe that we are in a position to best mitigate. I mentioned before that we use this layered approach——

Mr. WALDEN. Right.

Mr. DISTASIO [continuing]. To deal with these. But to the extent there was something that is yet not known to the industry that needs to be communicated, we would benefit by having specific and actionable information on that.

Mr. WALDEN. So let me go to our government witnesses here. Without getting into specific things we can't talk about here, are

the actions they are talking about they are doing, the sort of physical actions to deal with management of their systems and prevent against those threats, do they have as much knowledge as they need to know, need to have to deal with it without knowing specific time, place, type of attack?

Mr. MCCLELLAND. The distinction between classified and unclassified is who is the actor and what specific systems are being targeted.

The vectors back as far as the AURORA advisory, for instance, there was sufficient information and detail within that advisory for folks to be able to perform mitigation actions. And that advisory was not developed by the Commission. It was developed by DHS, DOE, and NERC and then issued to industry.

I think part of the question here is, is there a central agency that is responsible to get the information to the industry and then can hold industry accountable? Right now, all that we have is we have a coordination and a great partnership with DOE, DHS, and industry. But the advisories, the information that is conveyed is voluntary in nature.

Mr. WALDEN. And is it also your sense that those advisories, that information, those recommendations are not being acted upon to the extent they need to be acted upon? In other words, the systems aren't being upgraded or modified to deal with the threat, and they should be fully aware of what that threat is absent the classified piece of who it is and specific targets?

Mr. MCCLELLAND. Right. Congress asked the Commission to verify, for instance, the compliance with the AURORA advisory. And, on that basis, I would answer the question that, no, compliance is not sufficient. The Commission reached the conclusion that only if it can be compelled would we be able to assure that compliance has been executed for that.

Mr. WALDEN. Mr. Brown, let me give you the last 14 seconds.

Mr. BROWN. The more information the better. I will use New York State as an example. The single largest contingency we plan for is a 1,200 megawatt nuclear power plant going down, because that is our single largest worst thing that could happen. And at all times they maintain what is called spinning reserves, so if that plant goes down, everything is cool. Then they figure out the next biggest contingency and start planning for that.

The more information the more you can do those contingencies and be prepared for what happens to your system. Without the information, without a specific threat, they are going to be operating as if the situation was normal. And that is where I think you become most vulnerable at that point, when you are not prepared for two or three things happening at once, which if you knew that there was a threat of that you could plan your system around it.

So that is why the control area is even more important than the utilities when it comes to this. The utilities maintain their little footprint. But especially in the Northwest and in the Northeast, there are larger control areas that are looking at the system as a whole; and the larger a system you are looking at, the more contingencies you can use to address any problems that develop.

Mr. WALDEN. OK. My time has expired. Thank you very much for your testimony.

Mr. DISTASIO. Mr. Chairman.

Mr. MARKEY. Mr. DiStasio, yes.

Mr. DISTASIO. I would like to make one follow-up.

The industry does not agree that the information was specific and actionable, and what we would like to do is submit something for the record for the committee's benefit.

Mr. MARKEY. OK. That would be very helpful, as this hearing has been.

[The information appears at the conclusion of the hearing.]

Mr. MARKEY. We are going to focus very keenly in on all of the issues that have been identified here today. It is not lost on the committee that in a recent survey by the NERC of the generation owners in America that only one-third of them could identify a single critical asset to which the NERC cyber standards would apply. And so that, in and of itself, says something about this issue, that only one-third of all generators in America felt that they had any critical assets at all that should have protection.

So there is a big gap here. We have to find a way of closing it. And I think today you have really helped us to shape kind of the challenge for the committee: bulk power system versus the distribution system, cyber threats versus physical threats, emergency authority versus standards being set. So we have to walk through each of these issues, illuminated by the testimony that you have provided for us here today.

We thank all of you very much for your testimony. We want to stay very close to all of the stakeholders in this discussion so that we can ensure that we make the right decision in terms of the legislation, and we want to invite all the members of the committee as well to work with us so that we put together the best possible legislation.

The gentleman from Texas.

Dr. BURGESS. Mr. Chairman, I wonder if I might just ask one additional question while we are all gathered here.

Mr. MARKEY. The gentleman interrupted the chairman's concluding statement in order to make that unanimous consent request. So, without objection, the gentleman will be recognized to ask one question of the panel.

Dr. BURGESS. And I apologize, because I thought it was a soliloquy. I didn't realize it was the concluding statement.

On the issue of the——

Mr. MARKEY. When Chairmen Tauzin and Barton used to utter them, it was almost as if it was coming down from Mount Sinai as the 10 Commandments; and so I understand the different perspectives actually orient members differently when they hear the person with the gavel speaking.

Dr. BURGESS. It was just a general knowledge question on the issue of the solar interference.

Mr. McClelland, I guess this is for you. A couple of years ago, when I was working with the pilots union and flight attendant unions on trying to mitigate their exposure to in-flight radiation, I got the impression there was a predictive ability to these. Are we able to predict with any accuracy the sudden burst of solar activity?

Mr. MCCLELLAND. That is an excellent question, and it speaks to—I have had the same question sort of posed a different way: If the Commission did have emergency authority to be able to order mitigations against, say, solar magnetic activity, how could it exercise that when the warning would be so little?

There is a satellite deployed, it is the ACE satellite, that gives us about 15 to 30 minutes of warning for solar activity. And, in fact, some of the most massive solar storms in history have been with little or no sunspot activity. So sunspot activity is not a good predictor of the magnitude of solar storm that might occur. Fifteen or thirty minutes would be wholly inadequate unless the Commission had ordered mitigation plans be put into place first.

For instance, the EMP Commission said that a good way to mitigate against E3, this effect, would be to put a resistor in series with the transformer, maybe even a capacitor. Those could be put into place with 15 to 30 minutes. As long as the entities were practiced, they could be given that notice. And the thought would be that they will get more and more time, and they could switch those in to mitigate.

Dr. BURGESS. Thank you, Mr. Chairman.

Mr. MARKEY. The gentleman's time has expired.

We thank all the witnesses again. The big solar announcement today, of course, is that the President is down at Florida Power & Light making this big announcement about solar technology in Florida and its interrelationship with the smart grid. So, obviously, that focuses us on solar, on smart grid, on making sure we build this out correctly. Because obviously in this new distributed energy world that solar presents we need to continue to think through. But my congratulations to Florida Power & Light for that big breakthrough today with the President.

And, with that, this hearing is adjourned.

[Whereupon, at 11:37 a.m., the subcommittee was adjourned.]

[Material submitted for inclusion in the record follows:]

SMUD
SACRAMENTO MUNICIPAL UTILITY DISTRICT
The Power To Do More.

P.O. Box 15830, Sacramento, CA 95852-1830; 1-888-742-SMUD (7683)

November 10, 2009
GM 09-267

The Honorable Edward Markey
Chairman
Subcommittee on Energy and Environment
2125 Rayburn House Office Building
Washington, D.C. 20515-6115

The Honorable Fred Upton
Ranking Member
Subcommittee on Energy and Environment
2125 Rayburn House Office Building
Washington, D.C. 20515-6115

Dear Chairman Markey and Ranking Member Upton:

I am writing to follow-up on two issues raised during my testimony to the subcommittee for the hearing on October 27, 2009, entitled "Protecting the Electric Grid: H.R. 2165, the Bulk Power System Protection Act of 2009, and H.R. 2195."

The first issue was in response to a question from Representative Shimkus asking me to rank, in order of importance, four threats to the grid. I said that I would need to consult with the rest of the industry before responding, which I have subsequently done. The industry agrees to the following ranking, based on the likelihood of occurrence:

1) Cyber attacks
2) Solar flares
3) Radio frequency
4) Electro-magnetic pulse (EMP)

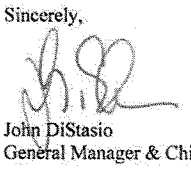
It is important to note that the industry is addressing all of these issues, but must weigh the likelihood of a threat occurring when allocating limited resources. Earlier this year, the North American Electric Reliability Corporation established a working group, in partnership with the Department of Energy, to analyze EMP threats and other high impact, low probability events like radio frequency attacks. It is my understanding that the working group intends to prepare an assessment that may lead to recommendations on needed technology research, development and investment to address EMP and other threats. Additional research conducted with industry participation is required to characterize the potential severity of an EMP attack on the nation's electric and related infrastructures, to provide a design basis for potential mitigation measures to protect electric system equipment from permanent damage, and to develop strategies for post-event system restoration.

The second issue is that of the industry's response to the "Aurora vulnerability." At the October 27 hearing, the FERC witness told the subcommittee that industry had received specific, actionable information to allow them to respond to the Aurora vulnerability. As the attached timeline makes clear, industry was not given sufficient, actionable information. In particular, the industry was not given sufficient actionable information by the federal government to clearly delineate the engineering basis of the Aurora vulnerability, and FERC's characterization of industry's response has been misleading.

The industry has prepared the attached timeline, beginning with the initial test conducted at a national lab, and dubbed "Aurora," which is intended to clarify what information industry was given and the industry's actions in response to that information.

I appreciate the opportunity to follow up on my testimony. Please do not hesitate to contact me should you have any questions.

Sincerely,



John DiStasio
General Manager & Chief Executive Officer

Attachment

Aurora Timeline

Late 2006 – Idaho National Lab conducts a test purportedly showing that remote cyber hackers can exploit a digital protection and control devices vulnerability by changing the phase settings of an electric power generator similar to those used in providing backup power to hospitals. This test is known as "Aurora."

Late February 2007/March 2007 -- The Department of Homeland Security (DHS) makes the North American Electric Reliability Corporation's Critical Infrastructure Protection Committee (NERC CIPC) aware of a potential cyber vulnerability which, if exploited by an attack, could have significant consequences. CIPC is specifically told that *it is not allowed* to distribute vulnerability information to utilities or to discuss the Aurora test with other individuals or organizations that were not present during the briefing.

March 20, 2007: A detailed briefing was convened for Canadian energy interests including electricity, oil and gas, and nuclear. Officials from Public Safety Canada, Natural Resources Canada, the Royal Canadian Mounted Police (RCMP) and the Integrated Threat Assessment Centre participated.

Spring 2007 – DHS forms "Tiger Team" of a small number of protection engineers to assist in developing mitigation measures to protect against an exploitation of the vulnerability.

May 2007 – NERC and DHS prepare draft mitigation measures on Aurora response, with FERC's knowledge. It is unclear whether or how the work of the industry "Tiger Team" factors into this draft. While the draft document is several pages long, it contains very little technical information about the vulnerability; the actual mitigation instructions consist of about five lines of text and do not contain specific instructions, as they are designed for distribution to a wide variety of utilities. While these are not classified, they are deemed "for official use only."

May 2007 – NERC asks the trade associations -- American Public Power Association (APPA), Edison Electric Institute (EEI), and National Rural Electric Cooperative Association (NRECA) -- to help distribute an Aurora Advisory containing the mitigation measures once the final document is ready.

June 7-8, 2007 – At the NERC CIPC meeting in Vancouver, Canada, a closed session of CIPC members and a DHS representative discuss the Aurora vulnerability in an effort to begin to understand the scope of the issue, and brainstorm actions that may be considered. DHS representative states that Aurora is a threat to (U.S.) national security.

June 21, 2007 – NERC distributes the "Aurora Advisory." Release of the Advisory was authorized by DOE and DHS on a "For Official Use Only" basis. Trade associations (APPA, EEI, NRECA and CEA) assist with making industry aware of the advisory, although NERC and DHS continue to imply that the document should be closely held, including suggesting that although the document is not officially classified it should be treated as such.

The mitigation measures focus on certain actions that the industry should take, but the problem is that the actual test on exploiting the vulnerability is classified at a higher level than that which industry representatives are given clearance by the government to access. (This is still the case today.) The mitigation measures provide no specifics on how the lab set up the test, what

protective settings were enabled/disabled, etc. The industry is only told the vulnerability "has been verified and it can happen."

It is easy to conclude from the Advisory that it is solely related to attacks on generators through generator substations and bulk power system (BPS) facilities in close electrical proximity to the generator. The Advisory is decidedly not clear that the underlying message, subsequently gleaned by the industry from the interactions delineated below, was that utilities should secure their electric control systems from unauthorized local and remote access.

June 21, 2007 -- DHS representatives hold a meeting in Ottawa with Public Safety Canada, Natural Resources Canada, Canadian Electricity Association (CEA) staff and CEA Security Infrastructure Protection Committee (SIPC) chair, among others, to review the Aurora test and mitigation measures. DHS clarifies their comment that Aurora becomes a threat to (U.S.) national security the moment that exploitation information is posted on the Internet.

June 28, 2007 – The Electric Power Supply Association (EPSA), after having received the Aurora Advisory from EEI, distributes to its members.

September 24, 2007 – Dramatized videotape of Aurora test (from December 2006) is leaked to major press outlets, resulting in CNN story and interview of senior DHS official. *Information about the test and vulnerability are still classified at a higher level than that which industry is cleared by the government to access.*

October 17, 2007 – House Homeland Security Committee convenes first of a series of hearings on the electric power industry's response to Aurora.

October 17, 2007 – Chairman of the House Homeland Security Committee, Bennie Thompson, and other members of Congress send letter to then-FERC Chairman Joe Kelliher requesting that FERC conduct an investigation of the industry's response to Aurora and general cybersecurity posture.

October 19, 2007 – NERC issues a survey to over 1,000 entities in U.S. and Canada requesting status of mitigation measures to date.

October 23, 2007 – FERC asks the Office of Management and Budget (OMB) to conduct a formal survey of generation and transmission owners/operators for the purpose of assessing progress in implementing the Aurora mitigation measures. Trade associations raise concerns due to Freedom of Information Act (FOIA)/Critical Electric Infrastructure Information (CEII) disclosure of detailed, highly sensitive data that would be collected in response to the survey.

January 8, 2008 – A small number of U.S. and Canadian electricity entities receive letters from House Homeland Security Committee Chairman Thompson and Emerging Threats Subcommittee Chairman Langevin requesting information regarding their discussions with NERC about implementation of the security recommendations contained in the June 21 Aurora Advisory.

January 2008 – U.S. trade associations file comments with OMB on FERC's request to survey utilities, expressing concerns about how the information will be secured, as well as whether such a volume of information will result in meaningful conclusions.

February 2008 – FERC withdraws its formal request to OMB and instead asks the utility industry trade associations (APPA, EEI, NRECA and EPSA) to facilitate interviews of certain of

their respective members concerning steps taken to respond to the Aurora Advisory. The trade associations provide listings of their members registered with NERC as generator owners, generator operators, transmission owners and transmission operators to FERC and FERC staff identify what they deem to be a representative sample of 30 specific industry members to be interviewed about compliance with the Aurora Advisory -- including 15 investor-owned utilities, nine rural electric co-operatives, three public power utilities, and three independent power producers. FERC determines that it wanted to interview 30 entities, but it was not limited to that number. The trade associations then contact these chosen entities and obtain their consent to meet voluntarily with FERC.

March–August 2008 – FERC conducts interviews with the 30 entities. Staff for each trade association, along with multiple staff from each interviewee, accommodate the interview process fully and openly. (Limited FERC technical staff resources cause the interview process to take nearly six months.) It becomes clear through this process that FERC staff do not think that the Aurora Advisory "went far enough." Thus, FERC evaluates each entity on what FERC thinks the advisory **should have covered** as opposed to what was actually was covered. FERC staff also takes the Aurora interviews as an opportunity to delve into the status of each utility's overall cyber-security readiness.

August 2008 -- Since the interviews covered more than just Aurora mitigation, the associations see the unrestricted dialogue between the government, with threat analysis expertise, and utilities, with operational expertise, as an opportunity to share this collaboration with other utilities. FERC at this point has not communicated any feedback from the interviews to the trade associations or the entities involved in the interviews (some of which have been completed several months before).

September 11, 2008 – FERC Chairman announces at a House Energy and Commerce subcommittee hearing, without having communicated same to the electric power industry, that 23 out of 30 interviewees have "failed" to mitigate effectively. Trade associations immediately request that FERC conduct follow-up meetings with the 30 utilities to provide FERC staff's assessment of whether the utility had, in FERC staff's view, successfully mitigated Aurora.

October 2008 – Trade associations begin coordinating follow–up meetings between 30 utilities and FERC staff. Timeline for follow-up meetings draws out due to FERC staff availability; entities that have been interviewed are anxious to hear how they were characterized and pressure trade associations for information and prompt meetings.

December 20, 2008 – CEA Vice President sends a letter to all Canadian utilities reminding them of the need to continue mitigation efforts of the Aurora vulnerability.

November 2008 – June 2009 – At the request of the trade associations, FERC conducts follow-up meetings with the 30 original interviewees. Several of these interviewees/companies assert that staff misinterpreted their mitigation steps. In follow-up calls, some FERC staff expresses belief that entities/companies are correct, but defer to staff interviewers. Despite several follow-up inquiries, staff fails to confirm that companies have taken sufficient mitigation measures. Despite these mixed signals, interviewees generally believe follow-up sessions were helpful to: clarify FERC's interpretation of the Advisory; receive FERC staff's perspective on cyber-security issues potentially affecting the electric utility industry; and hear about steps that utilities can and should take to secure their systems from unauthorized remote access.

Present (November 2009) – While the feedback above was provided, no general set of "lessons learned" from FERC or clarifications to the original intent of or recommended mitigation measures for the Aurora Advisory have been distributed to the industry as of this writing. A number of the 30 utilities remain unclear as to whether and why they are among the seven that "passed" or the 23 that "failed" based on FERC staff's classification.

Department of Energy
Washington, DC 20585

February 3, 2010

The Honorable Edward J. Markey
Chairman
Subcommittee on Energy and Environment
Committee on Energy and Commerce
U.S. House of Representatives
Washington, DC 20515

Dear Mr. Chairman:

On October 27, 2009, Patricia Hoffman, Principal Deputy Assistant Secretary, Office of Electricity Delivery and Energy Reliability, testified regarding "Protecting the Electric Grid: H.R. 2165, the Bulk Power System Protection Act of 2009, and H.R. 2195."

Enclosed is an answer to one question submitted by Representative Matsui to complete the hearing record.

If we can be of further assistance, please have your staff contact our Congressional Hearing Coordinator, Lillian Owen, at (202) 586-2031.

Sincerely,

Betty A. Nolan

Betty A. Nolan
Senior Advisor
Congressional and Intergovernmental Affairs

Enclosure

Printed with soy ink on recycled paper

QUESTION FROM REPRESENTATIVE MATSUI

Q1. In response to FERC's insufficient authority to guard against national security threats to the electric system, legislative initiatives have been proposed that would allow the Commission to act quickly to protect against cyber threats and other national security threats. Yet, we have heard from some in the industry that think that scope is too broad. Do you believe that we need to include cyber and other national security threats in the future legislation?

A1. The Department believes that additional authority may be warranted to protect the electric grid against cyber attacks in the event of a power grid emergency. A "power grid emergency" is defined as a situation that poses a high risk to the bulk power system that must be addressed urgently. The determination of a power grid emergency would be made by the Secretary of Energy, in consultation with the Secretary of Homeland Security, Attorney General, and the Director of National Intelligence. In making a determination of a power grid emergency, the Secretary of Energy will consider the existence of the following conditions:

- A known cyber vulnerability exists that may affect the bulk power system
- A threat actor is determined to have known or suspected intent, requisite resources, and capabilities to carry out the threat with a high likelihood
- If exploited, the vulnerability would result in significant consequences, including damage to assets and infrastructure, loss of life, and psychological damage.
- The situation presents an imminent risk to the bulk power system.

Should the Secretary of Energy declare a power grid emergency, the Federal Energy Regulatory Commission could be authorized to issue an Emergency Security

> Directive to owners and operators of the bulk power system without public disclosure, covering a specific period of time. Any directive should define security performance objectives and metrics for mitigating the identified threat, vulnerability, and/or potential consequences, and specify rules for satisfying the security performance objectives in accordance with the defined metrics within the defined time period of the power grid emergency. The Directive may alternatively be in the form of an alert that notifies owners and operators of a potentially serious cyber situation without specifying mandatory actions that must be taken. Specific methods for compliance shall be left to the discretion of the provider of bulk electric power, provided the security performance objectives are met.

Any directive should notify owners and operators of the bulk power system of the nature of the risk, consistent with the proper handling of classified and restricted information, direct the operators to investigate, take appropriate and corrective action, and report findings back to FERC within a specified time period. If required, the Directive would also direct owners and operators of the bulk power system, through North American Reliability Corporation, to develop mitigations, to test and validate such mitigations, and to recommend corrective actions. The Department of Energy could provide technical support in the development, testing, and validation of such mitigation measures.

Response of David Cook
Vice President and General Counsel
North American Electric Reliability Corporation
to Questions for the Record of the
October 27, 2009 Hearing before the
Subcommittee on Energy and the Environment
Committee on Energy and Commerce
on
"Protecting the Electric Grid: H.R. 2165, the Bulk Power System Protection Act of 2009, and H.R. 2195"

December 18, 2009

Question from the Honorable Doris Matsui:

1. It is our understanding that the cyber security standards approved by FERC took the industry approximately three years to develop. Yet we can all agree that cyber threats can attack us at any moment...hence a need for immediate responses. Mr. DiStasio mentioned in his testimony that "It is in the industry's best interests to protect against cyber security attacks."

In your testimony you also mentioned a need for proper industry consultation. How would you recommend getting industry input while maintaining an ability to respond quickly to threats?

Response:

It is important to distinguish between emergency directives as immediate responses to specific, imminent threats and standards that must apply for the long term to a wide variety of entities and circumstances. NERC has been supportive of legislation that would give an agency of the U.S. Federal Government the authority to act in the event of an imminent and specific cyber security threat. Any emergency directives put in place for the bulk power system must take into account the highly complex nature of the system and, to the extent possible, do no unintended harm. There is significant potential for an action on one part of the system to have unforeseen negative consequences on another part of the system. It is based on this concern that NERC supports appropriate coordination with industry experts during the development of any such emergency directives.

One possible solution would be to establish a consultative group of industry experts who, with appropriate security clearances, would be able to flag any issues that could arise during implementation or identify whether and where more technical information will be needed to appropriately execute the directive. This group should include a range of subject matter experts with experience operating and securing various components of the system.

NERC is prepared to assist the federal government in identifying these experts should such a framework be considered. NERC has already implemented a consultative process with industry

subject matter experts in the creation of its critical infrastructure protection alerts, bulletins, and guidance.

Long-term standards, such as those developed by NERC through its industry-based standards development process, should lay a strong foundation of sound security practices, but are not designed to address specific and emerging threats that are changing from week to week and day to day.

NERC adopted its first cyber security standards as Urgent Action Standard 1200 in August 2003, prior to passage of Section 215 of the Federal Power Act. NERC filed revisions to UA1200 in August 2006 as Version 1 of CIP-002 through CIP-009, which FERC approved in January 2008. NERC filed Version 2 of CIP-002 through CIP-009 in May 2009, responding to certain of FERC's directions for changes in Version 1. FERC approved Version 2 in September 2009, and gave further directives for changes to be completed within 90 days. On December 16, NERC's Board of Trustees approved Version 3 of the CIP standards addressing those 90-day directives. NERC continues to work on additional revisions to the CIP standards in response to earlier FERC directives.

As with emergency directives, any mandatory and enforceable standards that are put in place for the North American bulk power system for the long term must take into account the highly complex nature of the system and do no unintended harm. There is significant potential for an action on one part of the system to have unforeseen negative consequences on another part of the system. For that reason, NERC believes the development of long-term standards should continue to be done in a process that brings together the industry's technical expertise in a process that allows participation by all interested parties, from both the United States and Canada. NERC recently filed with FERC proposed changes to its standards development procedure to add a mechanism to develop standards through a process that maximizes the ability to use non-public information as part of the standards development process. It, too, would make use of a group of industry experts with appropriate security clearances for development of the standards.

○